(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－186358
（P2001－186358A）
(43)公開日　平成13年７月６日(2001.7.6)

Corr. US 7,003,667 B1

(51)Int.Cl.⁷	識別記号	FI		テーマコード（参考）
H04N 1/44		H04N 1/44		
H04L 9/08		H04L 9/00	601A	
			601B	
			601E	

審査請求　未請求　請求項の数123　ＯＬ　外国語出願　（全109頁）

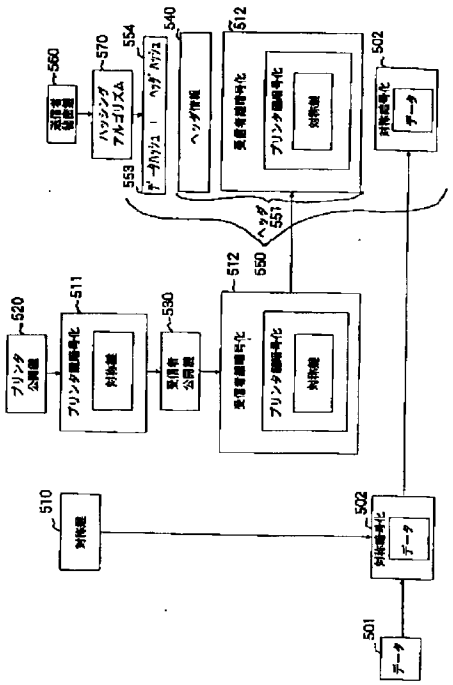
(21)出願番号　特願2000－305422(P2000－305422)
(22)出願日　平成12年10月４日(2000.10.4)
(31)優先権主張番号　０９／４１１０７０
(32)優先日　平成11年10月４日(1999.10.4)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号
(72)発明者　ロイス　イー．スリック
アメリカ合衆国　カリフォルニア州
92612，　アーバイン，　イノベーション　ドライブ　110　キヤノン　インフォメーション　システムズ，　インク．内
(74)代理人　100076428
弁理士　大塚　康徳　（外２名）

最終頁に続く

(54)【発明の名称】　画像出力方法及びその装置と記憶媒体

(57)【要約】　（修正有）
【課題】目的受信者に対して目的画像出力機器により確実に画像を安全送信して生成するシステムの提供。
【解決手段】受信印刷希望のデータ５０１を、先ずランダムに生成された第１の鍵の対称鍵５１０を用い、暗号化データ５０２を作成する。次にプリンタ公開鍵５２０を入手し、非対称暗号化アルゴリズムと共に利用して第２の対称鍵５１１を作成する。これは目的画像出力機器特定用となる。次いで受信公開鍵５３０を使用して第２の対称鍵５１１を再暗号化し、２回に亘り暗号化された第３の対称鍵５１２を作成する。これにより目的受信者の秘密鍵と目的プリンタの秘密鍵の特定組合せが得られる。これに印刷ジョブ情報を加えたヘッダ５５１、更にデータ完全性を保証するためのハッシュアルゴリズム５７０を用いたものと、対称暗号化データ５０２が加えられて、印刷ジョブ情報５５０を送信する。



1

【特許請求の範囲】

【請求項１】　データを使用して、目的受信者がいるときに目的画像出力機器で画像を生成する、前記目的画像出力機器へのデータの安全送信方法であって、

第１の鍵が第１の秘密鍵／公開鍵対の公開鍵であり、前記第１の秘密鍵／公開鍵対の秘密鍵が前記目的画像出力機器によって所有され、前記第２の鍵が第２の秘密鍵／公開鍵対の公開鍵であり、前記第２の秘密鍵／公開鍵対の秘密鍵が前記目的受信者によって所有されるものであり、前記第１の鍵及び第２の鍵を使用して前記データを２回にわたり暗号化する暗号化工程と、

前記２回にわたり暗号化された暗号化データを前記目的画像出力機器に送信する送信工程と、を有することを特徴とする方法。

【請求項２】　データを使用して、目的受信者がいるときに目的画像出力機器で画像を生成する、前記目的画像出力機器へのデータの安全送信方法であって、

第１の鍵を使用して前記データを暗号化する第１の暗号化工程と、

第２の鍵が第１の秘密鍵／公開鍵対の公開鍵であり、前記第１の秘密鍵／公開鍵対の秘密鍵が前記目的画像出力機器によって所有され、第３の鍵が第２の秘密鍵／公開鍵対の公開鍵であり、前記第２の秘密鍵／公開鍵対の秘密鍵が前記目的受信者によって所有されるもので、前記第２の鍵及び第３の鍵を使用して前記第１の鍵を２回にわたり暗号化する第２の暗号化工程と、

前記第１の暗号化工程で暗号化された暗号化データ及び前記２回にわたり暗号化された第１の鍵を前記目的画像出力機器に送信する送信工程と、を有することを特徴とする方法。

【請求項３】　前記第１の鍵がランダムに生成されることを特徴とする請求項２に記載の方法。

【請求項４】　第１の暗号化工程は、対称暗号化アルゴリズムを利用することを特徴とする請求項２に記載の方法。

【請求項５】　前記第２の暗号化工程は、非対称暗号化アルゴリズムを利用することを特徴とする請求項２に記載の方法。

【請求項６】　前記第２の暗号化工程では、前記第２の鍵を使用して前記第１の鍵を暗号化してから前記第３の鍵を使用して前記第１の鍵を暗号化することを特徴とする請求項２に記載の方法。

【請求項７】　前記第２の暗号化工程では、前記第３の鍵を使用して前記第１の鍵を暗号化してから前記第２の鍵を使用して前記第１の鍵を暗号化することを特徴とする請求項２に記載の方法。

【請求項８】　前記送信工程において、前記２回にわたり暗号化した第１の鍵がヘッダに含まれ、当該ヘッダが更に前記送信を開始した装置の識別に関係した情報を含むことを特徴とする請求項２に記載の方法。

2

【請求項９】　前記送信工程では、前記２回にわたり暗号化した第１の鍵がヘッダに含まれ、当該ヘッダが更に前記送信を開始した人物の識別に関係した情報を含むことを特徴とする請求項２に記載の方法。

【請求項１０】　ハッシングアルゴリズムを用いて前記ヘッダ及び前記暗号化データを処理し、ヘッダハッシュ及びデータハッシュを得るハッシング工程と、

前記第３の秘密鍵／公開鍵対の秘密鍵を用いて前記ヘッダハッシュ及び前記データハッシュにディジタル署名する署名工程とを更に有し、

前記第３の秘密鍵／公開鍵対の秘密鍵が前記送信を開始した人物だけによって所有され、前記送信工程において、署名付きヘッダハッシュ及び署名付きデータハッシュを送信することを特徴とする請求項９に記載の方法。

【請求項１１】　前記目的画像出力機器がプリンタであることを特徴とする請求項２に記載の方法。

【請求項１２】　前記目的画像出力機器がファクシミリ機器であることを特徴とする請求項２に記載の方法。

【請求項１３】　データを使用して、目的受信者がいるときに目的画像出力機器で画像を生成する、前記目的画像出力機器へのデータの安全送信方法であって、

第１の鍵を使用して前記データを暗号化する第１の暗号化工程と、

第２の鍵が第１の秘密鍵／公開鍵対の公開鍵であり、第１の秘密鍵／公開鍵対の秘密鍵が前記目的画像出力機器によって所有され、第３の鍵が第２の秘密鍵／公開鍵対の公開鍵であり、第２の秘密鍵／公開鍵対の秘密鍵が前記目的受信者によって所有されており、前記第２の鍵及び第３の鍵を使用して前記第１の鍵を２回にわたり暗号化する第２の暗号化工程と、

前記２回にわたる暗号化により暗号化された第１の鍵を含むヘッダを生成する生成工程と、

前記ヘッダを前記目的画像出力機器に送信する第１の送信工程と、

前記暗号化データの要求を前記目的画像出力機器から受信する受信工程と、

前記暗号化データを前記目的画像出力機器に送信する第２の送信工程と、を有することを特徴とする方法。

【請求項１４】　第１の送信工程では、前記ヘッダを電子メールで前記目的画像出力機器に送信することを特徴とする請求項１３に記載の方法。

【請求項１５】　前記生成工程で生成される前記ヘッダが更に前記暗号化データの記憶場所への参照を含み、前記暗号化データの要求により前記暗号化データの記憶場所が参照されることを特徴とする請求項１３に記載の方法。

【請求項１６】　２回にわたり暗号化した暗号化データを使用して、目的受信者がいるときに目的画像出力機器で画像を生成する方法であって、

前記暗号化データを受信する受信工程と、

第１の鍵が第１の秘密鍵／公開鍵対の秘密鍵であり、前記第１の秘密鍵／公開鍵対の秘密鍵が前記目的受信者によって所有され、第２の鍵が第２の秘密鍵／公開鍵対の秘密鍵であり、前記第２の秘密鍵／公開鍵対の秘密鍵が前記目的画像出力機器によって所有されており、前記第１の鍵及び第２の鍵を使用して前記暗号化データを２回にわたって復号する復号工程と、

前記復号工程で復号されたデータから画像を生成する画像生成工程と、を有することを特徴とする方法。

【請求項１７】　データを使用して、目的受信者がいるときに目的画像出力機器で画像を生成する、前記目的画像出力機器に送信されたデータから画像を生成する方法であって、

暗号化されたデータ及び２回にわたり暗号化された第１の鍵を受信する受信工程と、

第２の鍵が第１の秘密鍵／公開鍵対の秘密鍵であり、前記第１の秘密鍵／公開鍵対の秘密鍵が前記目的受信者によって所有され、第３の鍵が第２の秘密鍵／公開鍵対の秘密鍵であり、前記第２の秘密鍵／公開鍵対の秘密鍵が前記目的画像出力機器だけによって所有されており、前記第２の鍵及び第３の鍵を使用して前記２回にわたり暗号化された第１の鍵を２回に亙って復号する第１の復号工程と、

前記第１の復号工程で復号された第１の鍵を使用して前記暗号化データを復号する第２の復号工程と、

前記第２の復号工程で復号されたデータから画像を生成する画像生成工程と、を有することを特徴とする方法。

【請求項１８】　第１の復号工程が、非対称復号アルゴリズムを利用することを特徴とする請求項１７に記載の方法。

【請求項１９】　第２の復号工程が対称復号アルゴリズムを利用することを特徴とする請求項１７に記載の方法。

【請求項２０】　第１の復号工程が、前記第２の鍵を使用して前記２回にわたり暗号化された第１の鍵を復号してから、前記第３の鍵を使用して前記２回にわたり暗号化された第１の鍵を復号することを特徴とする請求項１７に記載の方法。

【請求項２１】　第１の復号工程が、前記第３の鍵を使用して前記２回にわたり暗号化された第１の鍵を復号してから、前記第２の鍵を使用して前記２回にわたり暗号化された第１の鍵を復号することを特徴とする請求項１７に記載の方法。

【請求項２２】　前記第３の鍵が前記目的画像出力機器の内部に含まれ、これによって前記第３の鍵が前記目的画像出力機器以外の装置によるアクセスから保護されることを特徴とする請求項１７に記載の方法。

【請求項２３】　前記第２の鍵が前記目的受信者が所有するスマートカードに含まれ、これによって前記第２の鍵が前記目的受信者以外の受信者から隠されることを特

徴とする請求項１７に記載の方法。

【請求項２４】　前記受信工程が更に、署名付きヘッダハッシュ及び署名付きデータハッシュを受信し、前記方法が更に前記署名付きヘッダハッシュ及び前記署名付きデータハッシュの正当性及び完全性を検証する検証工程を含むことを特徴とする請求項１７に記載の方法。

【請求項２５】　前記署名付きヘッダハッシュ又は前記署名付きデータハッシュが正当性及び完全性の検証に失敗した場合に、前記暗号化データに基づいて画像を出力することなく前記暗号化データを廃棄する工程を更に含むことを特徴とする請求項２４に記載の方法。

【請求項２６】　前記署名付きヘッダハッシュ又は前記署名付きデータハッシュが正当性及び完全性の検証に失敗した場合に、前記ヘッダの送信者に通知を送る工程を更に含むことを特徴とする請求項２５に記載の方法。

【請求項２７】　前記目的画像出力機器がプリンタであることを特徴とする請求項１７に記載の方法。

【請求項２８】　前記目的画像出力機器がファクシミリ機器であることを特徴とする請求項１７に記載の方法。

【請求項２９】　データを使用して、目的受信者がいるときに目的画像出力機器で前記画像を生成する、前記目的画像出力機器に送信されたデータから画像を生成する方法であって、

２回にわたり暗号化された第１の鍵を含むヘッダを受信する受信工程と、

前記ヘッダに対応する暗号化データの要求を送信する送信工程と、

前記ヘッダに対応する暗号化データを受信する受信工程と、

第２の鍵が第１の秘密鍵／公開鍵対の秘密鍵であり、前記第１の秘密鍵／公開鍵対の秘密鍵が前記目的受信者によって所有され、第３の鍵が第２の秘密鍵／公開鍵対の秘密鍵であり、前記第２の秘密鍵／公開鍵対の秘密鍵が前記目的画像出力機器によって所有される前記第２の鍵及び第３の鍵を使用して前記２回にわたり暗号化された第１の鍵を２回に亙って復号する第１の復号工程と、

復号された第１の鍵を使用して前記暗号化データを復号する第２の復号工程と、

復号されたデータから画像を生成する画像生成工程と、を有することを特徴とする方法。

【請求項３０】　前記受信工程で受信される前記ヘッダは電子メールで受信されることを特徴とする請求項２９に記載の方法。

【請求項３１】　前記ヘッダが更に、前記暗号化データの記憶場所への参照を含み、前記暗号化データを求める前記要求が前記暗号化データの記憶場所への参照を含むことを特徴とする請求項２９に記載の方法。

【請求項３２】　データを使用して、目的受信者がいるときに目的画像出力機器で画像を生成する、前記目的画像出力機器へのデータの安全送信装置であって、

実行可能プロセス工程及び前記画像用のデータを格納する領域を含むメモリと、
前記実行可能プロセス工程を実行するプロセッサとを備え、
前記実行可能プロセス工程は、
（ａ）第１の鍵が第１の秘密鍵／公開鍵対の公開鍵であり、前記第１の秘密鍵／公開鍵対の秘密鍵が前記目的画像出力機器によって所有され、第２の鍵が第２の秘密鍵／公開鍵対の公開鍵であり、前記第２の秘密鍵／公開鍵対の秘密鍵が前記目的受信者によって所有され、前記第１の鍵及び第２の鍵を使用して前記データを２回にわたり暗号化する暗号化工程と、
（ｂ）前記２回にわたり暗号化データを目的画像出力機器に送信する送信工程とを含むことを特徴とする装置。
【請求項３３】　データを使用して、目的受信者がいるときに目的画像出力機器で画像を生成する、前記目的画像出力機器へのデータの安全送信装置であって、
実行可能プロセス工程及び前記画像用のデータを格納する領域を含むメモリと、
前記実行可能プロセス工程を実行するプロセッサとを備え、
前記実行可能プロセス工程は、
（ａ）第１の鍵を使用して前記データを暗号化する第１の暗号化工程と、
（ｂ）第２の鍵が第１の秘密鍵／公開鍵対の公開鍵であり、前記第１の秘密鍵／公開鍵対の秘密鍵が前記目的画像出力機器によって所有され、第３の鍵が第２の秘密鍵／公開鍵対の公開鍵であり、前記第２の秘密鍵／公開鍵対の秘密鍵が前記目的受信者によって所有され、前記第２の鍵及び第３の鍵を使用して前記第１の鍵を２回にわたり暗号化する第２の暗号化工程と、
（ｃ）前記暗号化データ及び前記２回にわたり暗号化された第１の鍵を前記目的画像出力機器に送信する送信工程とを含むことを特徴とする装置。
【請求項３４】　前記第１の鍵がランダムに生成されることを特徴とする請求項３３に記載の装置。
【請求項３５】　前記第１の暗号化工程は、対称暗号化アルゴリズムを利用することを特徴とする請求項３３に記載の装置。
【請求項３６】　前記第２の暗号化工程は、非対称暗号化アルゴリズムを利用することを特徴とする請求項３３に記載の装置。
【請求項３７】　前記第２の暗号化工程が、前記第２の鍵を使用して前記第１の鍵を暗号化してから、前記第３の鍵を使用して前記第１の鍵を暗号化することを特徴とする請求項３３に記載の装置。
【請求項３８】　前記第２の暗号化工程は、前記第３の鍵を使用して前記第１の鍵を暗号化してから前記第２の鍵を使用して前記第１の鍵を暗号化することを特徴とする請求項３３に記載の装置。

【請求項３９】　前記送信工程では、前記２回にわたり暗号化された第１の鍵が前記ヘッダに含まれ、当該ヘッダが更に前記送信を開始した前記目的画像出力機器の識別に関係した情報を含むことを特徴とする請求項３３に記載の装置。
【請求項４０】　前記送信工程では、前記２回にわたり暗号化された第１の鍵が前記ヘッダに含まれ、当該ヘッダが更に前記送信を開始した人物の識別に関係した情報を含むことを特徴とする請求項３３に記載の装置。
【請求項４１】　前記実行可能プロセス工程は更に、
（ｄ）ハッシングアルゴリズムを用いて前記ヘッダ及び前記暗号化データを処理して、ヘッダハッシュ及びデータハッシュを得るハッシング工程と、
（ｅ）第３の秘密鍵／公開鍵対の秘密鍵を用いて前記ヘッダハッシュ及び前記データハッシュにディジタル署名する署名工程を含み、
前記第３の秘密鍵／公開鍵対の秘密鍵が前記送信を開始した人物によって所有され、前記送信工程では、更に前記署名付きヘッダハッシュ及び前記署名付きデータハッシュを送信することを特徴とする請求項４０に記載の装置。
【請求項４２】　前記安全送信装置がコンピュータであり、前記目的画像出力機器がプリンタであることを特徴とする請求項３３に記載の装置。
【請求項４３】　前記安全送信装置がコンピュータであり、前記目的画像出力機器がファクシミリ機器であることを特徴とする請求項３３に記載の装置。
【請求項４４】　前記安全送信装置が第１のファクシミリ機器であり、前記目的画像出力機器が第２のファクシミリ機器であることを特徴とする請求項３３に記載の装置。
【請求項４５】　データを使用して、目的受信者がいるときに目的画像出力機器で画像を生成する、前記目的画像出力機器へのデータの安全送信装置であって、
実行可能プロセス工程及び前記画像用のデータを格納する領域を含むメモリと、
前記実行可能プロセス工程を実行するプロセッサとを備え、
前記実行可能プロセス工程は、
（ａ）第１の鍵を使用して前記データを暗号化する第１の暗号化工程と、
（ｂ）第２の鍵が第１の秘密鍵／公開鍵対の公開鍵であり、前記第１の秘密鍵／公開鍵対の秘密鍵が前記目的画像出力機器によって所有され、第３の鍵が第２の秘密鍵／公開鍵対の公開鍵であり、前記第２の秘密鍵／公開鍵対の秘密鍵が前記目的受信者によって所有され、前記第２の鍵及び第３の鍵を使用して前記第１の鍵を２回にわたり暗号化する第２の暗号化工程と、
（ｃ）前記２回にわたり暗号化された第１の鍵を含むヘッダを生成する生成工程と、

（ｄ）前記ヘッダを前記目的画像出力機器に送信する第１の送信工程と、
（ｅ）前記暗号化データの要求を前記目的画像出力機器から受信する受信工程と、
（ｆ）前記暗号化データを前記目的画像出力機器に送信する第２の送信工程とを含むことを特徴とする装置。
【請求項４６】　前記第１の送信工程は、前記ヘッダを電子メールで前記目的画像出力機器に送信することを特徴とする請求項４５に記載の装置。
【請求項４７】　前記生成工程で生成される前記ヘッダは更に前記暗号化データの記憶場所への参照を含み、前記暗号化データの要求が前記暗号化データの記憶場所への参照を含むことを特徴とする請求項４５に記載の装置。
【請求項４８】　データを使用して、目的受信者がいるときに前記画像を生成する、送信されたデータから画像を生成する画像出力装置であって、
２回にわたり暗号化されたデータを受信する受信器と、
画像データから画像を生成する画像生成器と、
実行可能プロセス工程及びデータを格納する領域を含むメモリと、
前記実行可能プロセス工程を実行するプロセッサとを備え、
前記実行可能プロセスは、
（ａ）第１の鍵が第１の秘密鍵／公開鍵対の秘密鍵であり、前記第１の秘密鍵／公開鍵対の秘密鍵が前記目的受信者によって所有され、第２の鍵が第２の秘密鍵／公開鍵対の秘密鍵であり、前記第２の秘密鍵／公開鍵対の秘密鍵が前記目的画像出力機器によって所有され、前記第１の鍵及び第２の鍵を使用して前記２回にわたり暗号化されたデータを２回にわたり復号する復号工程と、
（ｂ）復号されたデータから画像を生成する画像生成工程とを有することを特徴とする画像出力装置。
【請求項４９】　データを使用して、目的受信者がいるときに前記画像を生成する、送信されたデータから画像を生成する画像出力装置であって、
暗号化されたデータ及び２回にわたり暗号化された第１の鍵を受信する受信器と、
画像データから画像を生成する画像生成器と、
実行可能プロセス工程及びデータを格納する領域を含むメモリと、
前記実行可能プロセス工程を実行するプロセッサとを備え、
前記実行可能プロセス工程は、
（ａ）第２の鍵が第１の秘密鍵／公開鍵対の秘密鍵であり、前記第１の秘密鍵／公開鍵対の秘密鍵が前記目的受信者によって所有され、第３の鍵が第２の秘密鍵／公開鍵対の秘密鍵であり、前記第２の秘密鍵／公開鍵対の秘密鍵が前記目的画像出力機器によって所有され、前記第２の鍵及び第３の鍵を使用して前記２回にわたり暗号化された第１の鍵を２回にわたり復号する第１の復号工程と、
（ｂ）復号された第１の鍵を使用して前記暗号化データを復号する第２の復号工程と、
（ｃ）復号されたデータから前記画像生成器を使用して画像を生成する画像生成工程を含むことを特徴とする画像出力装置。
【請求項５０】　前記第１の復号工程は、非対称復号アルゴリズムを利用することを特徴とする請求項４９に記載の画像出力装置。
【請求項５１】　前記第２の復号工程は、対称復号アルゴリズムを利用することを特徴とする請求項４９に記載の画像出力装置。
【請求項５２】　前記第１の復号工程は、前記第２の鍵を使用して前記第１の鍵を復号してから前記第３の鍵を使用して前記第１の鍵を復号することを特徴とする請求項４９に記載の画像出力装置。
【請求項５３】　前記第１の復号工程は、前記第３の鍵を使用して前記第１の鍵を復号してから、前記第２の鍵を使用して前記第１の鍵を復号することを特徴とする請求項４９に記載の画像出力装置。
【請求項５４】　前記第３の鍵が前記画像出力装置の内部に含まれ、前記第３の鍵が前記画像出力装置以外の装置によるアクセスから保護されることを特徴とする請求項４９に記載の画像出力装置。
【請求項５５】　前記第２の鍵は、前記目的受信者が所有するスマートカードの中に含まれ、前記第２の鍵が前記目的受信者以外の受信者から隠されることを特徴とする請求項４９に記載の画像出力装置。
【請求項５６】　前記受信器は、更に署名付きヘッダハッシュ及び署名付きデータハッシュを受信し、前記実行可能なプロセス工程は更に前記署名付きヘッダハッシュ及び前記署名付きデータハッシュの正当性及び完全性を検証する検証工程を含むことを特徴とする請求項４９に記載の画像出力装置。
【請求項５７】　前記実行可能プロセス工程は更に、前記署名付きヘッダハッシュ又は前記署名付きデータハッシュが正当性及び完全性の検証に失敗した場合に、画像を出力することなく前記暗号化データを廃棄する工程を含むことを特徴とする請求項５６に記載の画像出力装置。
【請求項５８】　前記実行可能プロセス工程は更に前記署名付きヘッダハッシュ又は前記署名付きデータハッシュが正当性及び完全性の検証に失敗した場合に、前記ヘッダの送信者に通知を送る工程を含むことを特徴とする請求項５７に記載の画像出力装置。
【請求項５９】　前記画像出力装置はプリンタであることを特徴とする請求項４９に記載の画像出力装置。
【請求項６０】　前記画像出力装置はファクシミリ機器であることを特徴とする請求項４９に記載の画像出力装

置。

【請求項６１】　データを使用して、目的受信者がいるときに前記画像を生成する、送信されたデータから画像を生成する画像出力装置であって、

２回にわたり暗号化された第１の鍵を含むヘッダを受信する受信器と、

画像データから画像を生成する画像生成器と、

実行可能プロセス工程及びデータを格納する領域を含むメモリと、

前記実行可能プロセス工程を実行するプロセッサとを備え、

前記実行可能プロセス工程は、

（ａ）前記ヘッダに対応する暗号化データの要求を送信する送信工程と、

（ｂ）前記ヘッダに対応する暗号化データを受信する受信工程と、

（ｃ）第２の鍵が第１の秘密鍵／公開鍵対の秘密鍵であり、前記第１の秘密鍵／公開鍵対の秘密鍵が前記目的受信者によって所有され、第３の鍵が第２の秘密鍵／公開鍵対の秘密鍵であり、前記第２の秘密鍵／公開鍵対の秘密鍵が前記目的画像出力機器によって所有され、前記第２の鍵及び第３の鍵を使用して前記２回にわたり暗号化された第１の鍵を２回にわたり復号する第１の復号工程と、

（ｄ）復号された前記第１の鍵を使用して前記暗号化データを復号する第２の復号工程と、

（ｅ）復号されたデータから画像を生成する画像生成工程とを含むことを特徴とする画像出力装置。

【請求項６２】　前記ヘッダは電子メールで受信されることを特徴とする請求項６１に記載の画像出力装置。

【請求項６３】　前記ヘッダは更に前記暗号化データの記憶場所への参照を含み、前記暗号化データの要求は前記暗号化データの記憶場所への参照を含むことを特徴とする請求項６１に記載の画像出力装置。

【請求項６４】　データを使用して、目的受信者がいるときに目的画像出力機器で画像を生成する、前記目的画像出力機器にデータを安全に送信するコンピュータ実行可能プロセス工程を格納したコンピュータ可読媒体であって、

前記コンピュータ実行可能プロセス工程は、

画像用のデータを生成するデータ生成工程と、

第１の鍵が第１の秘密鍵／公開鍵対の公開鍵であり、前記第１の秘密鍵／公開鍵対の秘密鍵が前記目的画像出力機器によって所有され、第２の鍵が第２の秘密鍵／公開鍵対の公開鍵であり、前記第２の秘密鍵／公開鍵対の秘密鍵が前記目的受信者によって所有され、前記第１の鍵及び第２の鍵を使用して前記データを２回にわたり暗号化する暗号化工程と、

前記２回にわたり暗号化されたデータを前記目的画像出力機器に送信する送信工程と、を有することを特徴とするコンピュータ可読媒体。

【請求項６５】　データを使用して、目的受信者がいるときに目的画像出力機器で画像を生成する、前記目的画像出力機器にデータを安全に送信するコンピュータ実行可能プロセス工程を格納したコンピュータ可読媒体であって、

前記コンピュータ実行可能プロセス工程は、

画像用のデータを生成するデータ生成工程と、

第１の鍵を使用して前記データを暗号化した暗号化データを生成する第１の暗号化工程と、

第２の鍵が第１の秘密鍵／公開鍵対の公開鍵であり、前記第１の秘密鍵／公開鍵対の秘密鍵が前記目的画像出力機器によって所有され、第３の鍵が第２の秘密鍵／公開鍵対の公開鍵であり、前記第２の秘密鍵／公開鍵対の秘密鍵が前記目的受信者によって所有され、前記第２の鍵及び第３の鍵を使用して前記第１の鍵を２回にわたり暗号化する第２の暗号化工程と、

前記暗号化データ及び前記２回にわたり暗号化された第１の鍵を前記目的画像出力機器に送信する送信工程と、を有することを特徴とするコンピュータ可読媒体。

【請求項６６】　前記第１の鍵がランダムに生成されることを特徴とする請求項６５に記載のコンピュータ可読媒体。

【請求項６７】　前記第１の暗号化工程は、対称暗号化アルゴリズムを利用することを特徴とする請求項６５に記載のコンピュータ可読媒体。

【請求項６８】　前記第２の暗号化工程は、非対称暗号化アルゴリズムを利用することを特徴とする請求項６５に記載のコンピュータ可読媒体。

【請求項６９】　前記第２の暗号化工程は、前記第２の鍵を使用して前記第１の鍵を暗号化してから前記第３の鍵を使用して前記第１の鍵を暗号化することを特徴とする請求項６５に記載のコンピュータ可読媒体。

【請求項７０】　前記第２の暗号化工程は、前記第３の鍵を使用して前記第１の鍵を暗号化してから前記第２の鍵を使用して前記第１の鍵を暗号化することを特徴とする請求項６５に記載のコンピュータ可読媒体。

【請求項７１】　前記送信工程で、前記２回にわたり暗号化された第１の鍵がヘッダに含まれ、ヘッダが更に、前記安全送信を開始した装置の識別に関係した情報を含む、請求項６５に記載のコンピュータ可読媒体。

【請求項７２】　前記送信工程では、前記２回にわたり暗号化された第１の鍵がヘッダに含まれ、当該ヘッダが更に前記送信を開始した人物の識別に関係した情報を含むことを特徴とする請求項６５に記載のコンピュータ可読媒体。

【請求項７３】　前記コンピュータ実行可能プロセス工程は更に、

ハッシングアルゴリズムを用いて前記ヘッダ及び前記暗号化データを処理して、ヘッダハッシュ及びデータハッ

シュを得るハッシング工程と、
第３の秘密鍵／公開鍵対の秘密鍵を用いて前記ヘッダハッシュ及び前記データハッシュにディジタル署名する署名工程とを含み、
前記第３の秘密鍵／公開鍵対の秘密鍵が前記送信を開始した人物によって所有され、前記送信工程が更に前記署名付きヘッダハッシュ及び前記署名付きデータハッシュを送信することを特徴とする請求項７２に記載のコンピュータ可読媒体。
【請求項７４】　前記目的画像出力機器はプリンタであることを特徴とする請求項６５に記載のコンピュータ可読媒体。
【請求項７５】　前記目的画像出力機器はファクシミリ機器であることを特徴とする請求項６５に記載のコンピュータ可読媒体。
【請求項７６】　データを使用して、目的受信者がいるときに目的画像出力機器で画像を生成する、前記目的画像出力機器にデータを安全に送信するコンピュータ実行可能プロセス工程を格納したコンピュータ可読媒体であって、
前記コンピュータ実行可能プロセス工程は、
画像用のデータを生成するデータ生成工程と、
第１の鍵を使用してデータを暗号化した暗号化データを生成する第１の暗号化工程と、
第２の鍵が第１の秘密鍵／公開鍵対の公開鍵であり、前記第１の秘密鍵／公開鍵対の秘密鍵が前記目的画像出力機器によって所有され、第３の鍵が第２の秘密鍵／公開鍵対の公開鍵であり、前記第２の秘密鍵／公開鍵対の秘密鍵が前記目的受信者によって所有され、前記第２の鍵及び第３の鍵を使用して前記第１の鍵を２回にわたり暗号化する第２の暗号化工程と、
前記２回にわたり暗号化された第１の鍵を含むヘッダを生成する生成工程と、
前記ヘッダを前記目的画像出力機器に送信する第１の送信工程と、
前記暗号化データの要求を前記目的画像出力機器から受信する受信工程と、
前記暗号化データを前記目的画像出力機器に送信する第２の送信工程と、を有することを特徴とするコンピュータ可読媒体。
【請求項７７】　前記第１の送信工程では、前記ヘッダを電子メールで前記目的画像出力機器に送信することを特徴とする請求項７６に記載のコンピュータ可読媒体。
【請求項７８】　前記生成工程で生成される前記ヘッダは更に前記暗号化データの記憶場所への参照を含み、前記暗号化データの要求が前記暗号化データの記憶場所への参照を含むことを特徴とする請求項７６に記載のコンピュータ可読媒体。
【請求項７９】　２回にわたる暗号化データを使用して、目的受信者がいるときに目的画像出力機器で前記画像を生成する、前記目的画像出力機器に送信された２回にわたり暗号化されたデータから画像を生成するコンピュータ実行可能プロセス工程を格納したコンピュータ可読媒体であって、
前記コンピュータ実行可能プロセス工程は、
２回にわたり暗号化された暗号化データを受信する受信工程と、
第１の鍵が第１の秘密鍵／公開鍵対の秘密鍵であり、前記第１の秘密鍵／公開鍵対の秘密鍵が前記目的受信者によって所有され、第２の鍵が第２の秘密鍵／公開鍵対の秘密鍵であり、前記第２の秘密鍵／公開鍵対の秘密鍵が前記目的画像出力機器によって所有され、前記第１の鍵及び第２の鍵を使用して前記暗号化データを２回にわたり復号する復号工程と、
復号されたデータから画像を生成する画像生成工程と、を有することを特徴とするコンピュータ可読媒体。
【請求項８０】　データを使用して、目的受信者がいるときに目的画像出力機器で前記画像を生成する、前記目的画像出力機器に送信されたデータから画像を生成するコンピュータ実行可能プロセス工程を格納したコンピュータ可読媒体であって、
前記コンピュータ実行可能プロセス工程は、
暗号化されたデータ及び２回にわたって暗号化された第１の鍵を受信する受信工程と、
第２の鍵が第１の秘密鍵／公開鍵対の秘密鍵であり、前記第１の秘密鍵／公開鍵対の秘密鍵が前記目的受信者によって所有され、第３の鍵が第２の秘密鍵／公開鍵対の秘密鍵であり、前記第２の秘密鍵／公開鍵対の秘密鍵が前記目的画像出力機器によって所有され、前記第２の鍵及び第３の鍵を使用して前記２回にわたり暗号化された第１の鍵を２回にわたって復号する第１の復号工程と、
復号された第１の鍵を使用して前記暗号化データを復号する第２の復号工程と、
復号されたデータから画像を生成する画像生成工程と、を有することを特徴とするコンピュータ可読媒体。
【請求項８１】　前記第１の復号工程は、非対称復号アルゴリズムを利用することを特徴とする請求項８０に記載のコンピュータ可読媒体。
【請求項８２】　前記第２の復号工程は、対称復号アルゴリズムを利用することを特徴とする請求項８０に記載のコンピュータ可読媒体。
【請求項８３】　前記第１の復号工程は、前記第２の鍵を使用して前記２回にわたり暗号化された第１の鍵を復号してから前記第３の鍵を使用して前記２回にわたり暗号化された第１の鍵を復号することを特徴とする請求項８０に記載のコンピュータ可読媒体。
【請求項８４】　前記第１の復号工程は、前記第３の鍵を使用して前記２回にわたり暗号化された第１の鍵を復号してから、前記第２の鍵を使用して前記２回にわたり暗号化された第１の鍵を復号することを特徴とする請求

項８０に記載のコンピュータ可読媒体。

【請求項８５】　前記第３の鍵が前記目的画像出力機器の内部に含まれ、前記第３の鍵が前記目的画像出力機器以外の装置によるアクセスから保護されることを特徴とする請求項８０に記載のコンピュータ可読媒体。

【請求項８６】　前記第２の鍵は、前記目的受信者が所有するスマートカードに含まれ、前記第２の鍵は前記目的受信者以外の受信者から隠されることを特徴とする請求項８０に記載のコンピュータ可読媒体。

【請求項８７】　前記受信工程では更に署名付きヘッダハッシュ及び署名付きデータハッシュを受信し、前記コンピュータ実行可能プロセス工程は更に、前記署名付きヘッダハッシュ及び前記署名付きデータハッシュの正当性及び完全性を検証する検証工程を含むことを特徴とする請求項８０に記載のコンピュータ可読媒体。

【請求項８８】　前記署名付きヘッダハッシュ又は前記署名付きデータハッシュが正当性及び完全性の検証に失敗した場合に、前記暗号化データに基づいて画像を出力することなく前記暗号化データを廃棄する工程を更に含むことを特徴とする請求項８７に記載のコンピュータ可読媒体。

【請求項８９】　前記署名付きヘッダハッシュ又は前記署名付きデータハッシュが正当性及び完全性の検証に失敗した場合に、前記ヘッダの送信者に通知を送る工程を更に含むことを特徴とする請求項８８に記載のコンピュータ可読媒体。

【請求項９０】　前記目的画像出力機器はプリンタであることを特徴とする請求項８０に記載のコンピュータ可読媒体。

【請求項９１】　前記目的画像出力機器はファクシミリ機器であることを特徴とする請求項８０に記載のコンピュータ可読媒体。

【請求項９２】　データを使用して、目的受信者がいるときに目的画像出力機器で前記画像を生成する、前記目的画像出力機器に送信されたデータから画像を生成するコンピュータ実行可能プロセス工程を格納したコンピュータ可読媒体であって、

前記コンピュータ実行可能プロセス工程は、

２回にわたって暗号化された第１の鍵を含むヘッダを受信する受信工程と、

前記ヘッダに対応する暗号化データの要求を送信する送信工程と、

前記ヘッダに対応する暗号化データを受信する受信工程と、

第２の鍵が第１の秘密鍵／公開鍵対の秘密鍵であり、前記第１の秘密鍵／公開鍵対の秘密鍵が前記目的受信者によって所有され、第３の鍵が第２の秘密鍵／公開鍵対の秘密鍵であり、前記第２の秘密鍵／公開鍵対の秘密鍵が前記目的画像出力機器によって所有され、前記第２の鍵及び第３の鍵を使用して前記２回にわたり暗号化された第１の鍵を２回にわたって復号する第１の復号工程と、

復号された前記第１の鍵を使用して前記暗号化データを復号する第２の復号工程と、

復号されたデータから画像を生成する画像生成工程と、

を有することを特徴とするコンピュータ可読媒体。

【請求項９３】　前記受信工程では、前記ヘッダが電子メールで受信されることを特徴とする請求項９２に記載のコンピュータ可読媒体。

【請求項９４】　前記ヘッダは更に前記暗号化データの記憶場所への参照を含み、前記暗号化データの要求は前記暗号化データの記憶場所への参照を含むことを特徴とする請求項９２に記載のコンピュータ可読媒体。

【請求項９５】　データを使用して、目的受信者がいるときに目的プリンタで画像を生成する、前記目的プリンタにデータを安全に送信するプリンタドライバであって、

画像用のデータを生成するデータ生成コードと、

第１の鍵が第１の秘密鍵／公開鍵対の公開鍵であり、前記第１の秘密鍵／公開鍵対の秘密鍵が前記目的プリンタによって所有され、第２の鍵が第２の秘密鍵／公開鍵対の公開鍵であり、前記第２の秘密鍵／公開鍵対の秘密鍵が前記目的受信者によって所有され、前記第１の鍵及び第２の鍵を使用して前記データを２回にわたって暗号化する暗号化コードと、

前記２回にわたる暗号化データを前記目的プリンタに送信する送信コードと、を有することを特徴とするプリンタドライバ。

【請求項９６】　データを使用して、目的受信者がいるときに目的プリンタで画像を生成する、前記目的プリンタにデータを安全に送信するプリンタドライバであって、

画像用のデータを生成するデータ生成コードと、

第１の鍵を使用して前記データを暗号化して暗号化データを生成する第１の暗号化コードと、

第２の鍵が第１の秘密鍵／公開鍵対の公開鍵であり、前記第１の秘密鍵／公開鍵対の秘密鍵が前記目的プリンタによって所有され、第３の鍵が第２の秘密鍵／公開鍵対の公開鍵であり、前記第２の秘密鍵／公開鍵対の秘密鍵が前記目的受信者によって所有され、前記第２の鍵及び第３の鍵を使用して前記第１の鍵を２回にわたって暗号化する第２の暗号化コードと、

前記暗号化データ及び前記２回にわたり暗号化された第１の鍵を前記目的プリンタに送信する送信コードと、を有することを特徴とするプリンタドライバ。

【請求項９７】　前記第１の鍵は、ランダムに生成されることを特徴とする請求項９６に記載のプリンタドライバ。

【請求項９８】　前記第１の暗号化コードが対称暗号化アルゴリズムを利用する、請求項９６に記載のプリンタドライバ。

15

【請求項９９】　第２の暗号化コードは、非対称暗号化アルゴリズムを利用することを特徴とする請求項９６に記載のプリンタドライバ。

【請求項１００】　前記第２の暗号化コードは、前記第２の鍵を使用して前記第１の鍵を暗号化してから前記第３の鍵を使用して前記第１の鍵を暗号化することを特徴とする請求項９６に記載のプリンタドライバ。

【請求項１０１】　前記第２の暗号化コードは、前記第３の鍵を使用して前記第１の鍵を暗号化してから前記第２の鍵を使用して前記第１の鍵を暗号化することを特徴とする請求項９６に記載のプリンタドライバ。

【請求項１０２】　前記２回にわたり暗号化された第１の鍵がヘッダに含まれ、当該ヘッダが更に前記送信を開始した人物の識別に関係した情報を含むことを特徴とする請求項９６に記載のプリンタドライバ。

【請求項１０３】　前記ヘッダが更に、署名付きヘッダハッシュ及び署名付きデータハッシュを含み、前記プリンタドライバは更に前記署名付きヘッダハッシュ及び前記署名付きデータハッシュの正当性及び完全性を検証する検証コードを含むことを特徴とする請求項１０２に記載のプリンタドライバ。

【請求項１０４】　前記署名付きヘッダハッシュと前記署名付きデータハッシュのうちの一方が正当性及び完全性の検証に失敗した場合に、前記ヘッダの送信者に通知する送信コードを更に含むことを特徴とする請求項１０３に記載のプリンタドライバ。

【請求項１０５】　データを使用して、目的受信者がいるときに目的プリンタで画像を生成する、前記目的プリンタにデータを安全に送信するプリンタドライバであって、

画像用のデータを生成するデータ生成コードと、

第１の鍵を使用して前記データを暗号化した暗号化データを生成する第１の暗号化コードと、

第２の鍵が第１の秘密鍵／公開鍵対の公開鍵であり、前記第１の秘密鍵／公開鍵対の秘密鍵が前記目的プリンタによって所有され、第３の鍵が第２の秘密鍵／公開鍵対の公開鍵であり、前記第２の秘密鍵／公開鍵対の秘密鍵が前記目的受信者によって所有され、前記第２の鍵及び第３の鍵を使用して前記第１の鍵を２回にわたって暗号化する第２の暗号化コードと、

前記２回にわたり暗号化された前記第１の鍵を含むヘッダを生成する生成コードと、

前記ヘッダを前記目的プリンタに送信する第１の送信コードと、

前記暗号化データの要求を前記目的プリンタから受信する受信コードと、

前記暗号化データを前記目的プリンタに送信する第２の送信コードと、を有することを特徴とするプリンタドライバ。

【請求項１０６】　前記第１の送信コードは、前記ヘッダを電子メールで前記目的プリンタに送信することを特徴とする請求項１０５に記載のプリンタドライバ。

16

【請求項１０７】　前記生成コードにより生成される前記ヘッダが更に前記暗号化データの記憶場所への参照を含み、前記暗号化データの要求は前記暗号化データの記憶場所への参照を含むことを特徴とする請求項１０５に記載のプリンタドライバ。

【請求項１０８】　２回にわたり暗号化された暗号化データを使用して、目的受信者がいるときに目的画像出力機器で画像を生成する、前記目的画像出力機器に送信された暗号化されたデータから画像を生成するコンピュータ可読媒体上に格納されたコンピュータ実行可能プロセス工程であって、

２回にわたり暗号化された暗号化データを受信する受信コードと、

第１の鍵が第１の秘密鍵／公開鍵対の秘密鍵であり、前記第１の秘密鍵／公開鍵対の秘密鍵が前記目的受信者によって所有され、第２の鍵が第２の秘密鍵／公開鍵対の秘密鍵であり、前記第２の秘密鍵／公開鍵対の秘密鍵が前記目的画像出力機器によって所有され、前記第１の鍵及び第２の鍵を使用して前記暗号化データを２回にわたって復号する復号コードと、

復号されたデータから画像を生成する画像生成コードと、を有することを特徴とするコンピュータ実行可能プロセス工程。

【請求項１０９】　データを使用して、目的受信者がいるときに目的画像出力機器で画像を生成する、前記目的画像出力機器に送信されたデータから画像を生成するコンピュータ可読媒体上に格納されたコンピュータ実行可能プロセス工程であって、

暗号化されたデータ及び２回にわたって暗号化された第１の鍵を受信する受信コードと、

第２の鍵が第１の秘密鍵／公開鍵対の秘密鍵であり、前記第１の秘密鍵／公開鍵対の秘密鍵が前記目的受信者によって所有され、第３の鍵が第２の秘密鍵／公開鍵対の秘密鍵であり、前記第２の秘密鍵／公開鍵対の秘密鍵が前記目的画像出力機器によって所有され、前記第２の鍵及び第３の鍵を使用して前記２回にわたって暗号化された第１の鍵を２回にわたって復号する第１の復号コードと、

復号された前記第１の鍵を使用して前記暗号化データを復号する第２の復号コードと、

復号されたデータから画像を生成する画像生成コードと、を有することを特徴とするコンピュータ実行可能プロセス工程。

【請求項１１０】　前記第１の復号コードは、非対称復号アルゴリズムを利用することを特徴とする請求項１０９に記載のコンピュータ実行可能プロセス工程。

【請求項１１１】　前記第２の復号コードは、対称復号アルゴリズムを利用することを特徴とする請求項１０９

に記載のコンピュータ実行可能プロセス工程。

【請求項１１２】　前記第１の復号コードは、前記第２の鍵を使用して前記２回にわたり暗号化された第１の鍵を復号してから、前記第３の鍵を使用して前記２回にわたり暗号化された第１の鍵を復号することを特徴とする請求項１０９に記載のコンピュータ実行可能プロセス工程。

【請求項１１３】　前記第１の復号コードは、前記第３の鍵を使用して前記２回にわたり暗号化された第１の鍵を復号してから、前記第２の鍵を使用して前記２回にわたり暗号化された第１の鍵を復号することを特徴とする請求項１０９に記載のコンピュータ実行可能プロセス工程。

【請求項１１４】　前記第３の鍵は前記目的画像出力機器の内部に含まれ、前記第３の鍵が前記目的画像出力機器以外の装置によるアクセスから保護されることを特徴とする請求項１０９に記載のコンピュータ実行可能プロセス工程。

【請求項１１５】　前記第２の鍵は、前記目的受信者が所有するスマートカードに含まれ、前記第２の鍵が前記目的受信者以外の受信者から隠されることを特徴とする請求項１０９に記載のコンピュータ実行可能プロセス工程。

【請求項１１６】　前記受信コードは更に、署名付きヘッダハッシュ及び署名付きデータハッシュを受信し、
前記コンピュータ実行可能プロセス工程は更に、前記署名付きヘッダハッシュ及び前記署名付きデータハッシュの正当性及び完全性を検証する検証コードを含むことを特徴とする請求項１０９に記載のコンピュータ実行可能プロセス工程。

【請求項１１７】　前記署名付きヘッダハッシュ又は前記署名付きデータハッシュが正当性及び完全性の検証に失敗した場合に、前記暗号化データに基づいて画像を出力することなく前記暗号化データを廃棄するコードを更に含むことを特徴とする請求項１１６に記載のコンピュータ実行可能プロセス工程。

【請求項１１８】　前記署名付きヘッダハッシュ又は前記署名付きデータハッシュが正当性及び完全性の検証に失敗した場合に、前記ヘッダの送信者に通知を送るコードを更に含むことを特徴とする請求項１１７に記載のコンピュータ実行可能プロセス工程。

【請求項１１９】　前記目的画像出力機器はプリンタであることを特徴とする請求項１０９に記載のコンピュータ実行可能プロセス工程。

【請求項１２０】　前記目的画像出力機器がファクシミリ機器であることを特徴とする請求項１０９に記載のコンピュータ実行可能プロセス工程。

【請求項１２１】　データを使用して、目的受信者がいるときに目的画像出力機器で画像を生成する、前記目的画像出力機器に送信されたデータから画像を生成するコンピュータ可読媒体上に格納されたコンピュータ実行可能プロセス工程であって、
２回に亙って暗号化された第１の鍵を含むヘッダを受信する受信コードと、
前記ヘッダに対応する暗号化データの要求を送信する送信コードと、
前記ヘッダに対応する暗号化データを受信する受信コードと、
第２の鍵が第１の秘密鍵／公開鍵対の秘密鍵であり、前記第１の秘密鍵／公開鍵対の秘密鍵が前記目的受信者によって所有され、第３の鍵が第２の秘密鍵／公開鍵対の秘密鍵であり、前記第２の秘密鍵／公開鍵対の秘密鍵が前記目的画像出力機器によって所有され、前記第２の鍵及び第３の鍵を使用して前記２回にわたり暗号化された第１の鍵を２回にわたって復号する第１の復号コードと、
復号された前記第１の鍵を使用して前記暗号化データを復号する第２の復号コードと、
復号されたデータから画像を生成する画像生成コードと、を有することを特徴とするコンピュータ実行可能プロセス工程。

【請求項１２２】　前記ヘッダが電子メールで受信されることを特徴とする請求項１２１に記載のコンピュータ実行可能プロセス工程。

【請求項１２３】　前記ヘッダは更に前記暗号化データの記憶場所への参照を含み、前記暗号化データの要求が前記暗号化データの記憶場所への参照を含むことを特徴とする請求項１２１に記載のコンピュータ実行可能プロセス工程。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、目的の受信者（目的受信者）がいるときにだけ目的の画像出力装置（目的画像出力機器）によって画像を生成することができる安全印刷（secure printing）を実行する画像出力方法、装置及びコンピュータ可読媒体に関するものである。詳細には本発明は、目的画像出力機器と目的受信者の両方によって供給される情報を使用しないと復号することができない印刷データの暗号化に関する。

【０００２】

【従来の技術】ネットワーク化されたオフィス環境では、ネットワーク内の１つの場所にあるコンピュータが生成した印刷ジョブを、別の場所にある画像出力装置が印刷することができる。その印刷ジョブが秘密ないし機密情報を含む場合には、ネットワーク内のいくつかあるポイントのうちの１つで印刷ジョブが無許可で傍受される心配が生じる。具体的には、単純なネットワーク・スヌーピング・ツールを実行中のコンピュータシステムなどのネットワーク上の装置によって印刷ジョブが傍受される可能性がある。

【０００３】更に、印刷された出力が無許可で閲覧される心配も生じる。その印刷された文書は、目的受信者が文書を受け取るために画像出力装置に到着する前に、たまたまその近くに居た人なら誰でも見ることができる。

【０００４】同様の問題はファクシミリ送信でも起こり得る。送信が傍受される可能性があり、また、目的受信者よりも先に送信先ファクシミリ機に到着した人なら誰でもそのファクシミリ文書を見ることができる。

【０００５】

【発明が解決しようとする課題】従って、印刷又はファクシミリ送信された文書を、目的受信者がいるときにだけ目的画像出力機器で生成することができる構成が求められている。

【０００６】

【課題を解決するための手段】本発明は、ランダムに生成された対称鍵を用い対称暗号化アルゴリズムを使用して印刷データを暗号化し、次いで、目的受信者がいるときにだけ目的画像出力機器によって復元することができるような方法でこの対称鍵を暗号化することによって、上記の必要性に対処する。対称鍵の暗号化は、非対称暗号化（すなわち公開／秘密鍵対）アルゴリズムによって実行する。対称鍵は、目的受信者の公開鍵と目的画像出力機器の公開鍵の両方を使用し２回にわたって暗号化する。次いで、暗号化された印刷データ及び暗号化されたランダムに生成された対称鍵を目的画像出力機器に送信する。

【０００７】文書の画像を生成するためには、目的画像出力機器の秘密鍵と目的受信者の秘密鍵の両方を使用してこの２回にわたり暗号化された対称鍵を復号する。好ましくは、目的受信者の秘密鍵が目的受信者によって個人的に供給されなければならない。対称鍵を復号した後、この復号された対称鍵を使用して印刷データを復号し、その復号された印刷データに基づいて画像を目的画像出力機器によって出力する。

【０００８】上記の構成の結果、目的受信者の秘密鍵と目的画像出力機器の秘密鍵の両方を使用しないと対称鍵は回復することができない。従って、これらの秘密鍵が、それぞれ目的受信者及び目的画像出力機器だけによって所有されている限り、対称鍵は、目的受信者がいる時にだけ目的画像出力機器でしか復元することができない。印刷データを復号するためにはこの対称鍵が必要なため、印刷データの画像は、目的受信者がいるときにだけ目的画像出力機器でしか印刷することができない。

【０００９】従って本発明の一態様は、プリンタ、ファクシミリ機器などの目的画像出力機器へのデータの安全送信に関する。このデータを使用して、目的受信者がいるときにだけ目的画像出力機器で画像を生成することができる。第１の鍵を使用してデータを暗号化する。次いで、まず第２の鍵、続いて第３の鍵を使用して第１の鍵を２回にわたって暗号化する。第２の鍵は、第１の秘密

鍵／公開鍵対の公開鍵であり、第１の秘密鍵／公開鍵対の秘密鍵は、その目的画像出力機器だけで所有される。第３の鍵は第２の秘密鍵／公開鍵対の公開鍵であり、第２の秘密鍵／公開鍵対の秘密鍵は本来、その目的受信者だけで所有される。次いで、暗号化データ及び２回にわたり暗号化された第１の鍵の双方を目的画像出力機器に送信する。

【００１０】この第１の鍵は、ランダムに生成されることが好ましい。更に、第１の鍵を用いたデータの暗号化は、対称暗号化アルゴリズムを使用して実行されることが好ましく、第２及び第３の鍵を用いた第１の鍵の暗号化は、非対称暗号化アルゴリズムを使用して実行されることが好ましい。

【００１１】更に、第２及び第３の鍵を使用した第１の鍵の暗号化の順序を逆にすることができる。例えば、第２の鍵を使用して第１の鍵を暗号化してから、第３の鍵を使用した第１の鍵の第２の暗号化を実施することができる。或いは、第３の鍵を使用して第１の鍵を暗号化してから、第２の鍵を使用した第１の鍵の第２の暗号化を実施してもよい。

【００１２】２回にわたり暗号化された第１の鍵は、送信者及び受信者の識別に関係したその他の情報とともにヘッダに含まれることが好ましい。好ましい実施の形態では、この方法が更に、暗号ハッシングアルゴリズムを適用することによってヘッダ及び暗号化データを処理し、ヘッダハッシュ及びデータハッシュを得る工程、及び第４の鍵を用いてヘッダハッシュ及びデータハッシュにディジタル署名する工程を含む。第４の鍵は、第３の秘密鍵／公開鍵対の秘密鍵であり、第３の秘密鍵／公開鍵対の秘密鍵は本来、データ送信を開始した人物だけに所有される。この送信工程が、署名付きヘッダハッシュ及び署名付きデータハッシュを暗号化データ、及び２回にわたり暗号化された第１の鍵と一緒に送信することが好ましい。

【００１３】上記の構成によって、画像を生成するためのデータを画像出力装置に送信し、これによってこの画像を、目的受信者がいるときにだけ、目的画像出力機器によって印刷することができる。

【００１４】他の態様では、本発明は、プリンタ、ファクシミリ機などの目的画像出力機器に送信されたデータからの画像の生成、又はこのような装置自体に関する。このデータを使用して、目的受信者がいる時にだけ目的画像出力機器で画像を生成することができる。暗号化されたデータ及び２回にわたって暗号化された第１の鍵を目的画像出力機器が受信する。第２の鍵及び第３の鍵を使用して暗号化第１の鍵を２回にわたって復号する。第２の鍵は第１の秘密鍵／公開鍵対の秘密鍵であり、第１の秘密鍵／公開鍵対の秘密鍵は本来、目的受信者だけで所有される。第３の鍵は、第２の秘密鍵／公開鍵対の秘密鍵であり、第２の秘密鍵／公開鍵対の秘密鍵は本来、

目的画像出力機器だけで所有される。暗号化第１の鍵を２回にわたって復号した後、その復号された第１の鍵を使用して暗号化データを復号し、復号されたデータから画像を目的画像出力機器によって生成する。

【００１５】第２及び第３の鍵を使用した第１の鍵の復号は、非対称復号アルゴリズムを使用して実行されることが好ましい。復号された第１の鍵を使用した暗号化データの復号は、対称復号アルゴリズムを使用して実行されることが好ましい。

【００１６】第１の鍵の暗号化の順序に応じ、第２の鍵を使用して第１の鍵を復号してから、第３の鍵を使用して第１の鍵を復号することができる。或いは、第３の鍵を使用して第１の鍵を復号してから、第２の鍵を使用して第１の鍵を復号することができる。

【００１７】好ましい実施の形態では、第２の鍵が、目的受信者が所有するスマートカードの中に含まれる。従って第２の鍵は本来、目的受信者の許可がある場合に限ってアクセス可能である。同様に、第３の鍵は、目的画像出力機器の内部に保持されたスマートチップの中に含まれ、これによって目的画像出力機器以外の装置によるアクセスから保護されることが好ましい。

【００１８】目的画像出力機器が更に、送信者及び受信者の識別に関係した情報を含むヘッダを受信することが好ましい。更に好ましい実施の形態では、前記受信工程が更に、署名付きヘッダハッシュ及び署名付きデータハッシュを受信する工程を含む。第３の公開鍵／秘密鍵対の公開鍵である第４の鍵を使用して、署名付きヘッダハッシュ及び署名付きデータハッシュの正当性を検証することが好ましい。第３の公開鍵／秘密鍵対の秘密鍵は本来、目的画像出力機器が受信したデータの送信を開始した人物によってのみ所有される。署名付きヘッダハッシュ又は署名付きデータハッシュが正当性の検証に失敗した場合には、暗号化データを廃棄することが好ましい。検証に成功した場合には、暗号ハッシングアルゴリズムをヘッダ及び暗号化データに適用することによって、署名付きヘッダハッシュ及び署名付きデータハッシュの完全性を検証する。署名付きヘッダハッシュ又は署名付きデータハッシュが完全性の検証に失敗した場合には、暗号化データを廃棄することが好ましい。

【００１９】上記の構成によって、画像出力装置に送信されたデータがその画像出力装置に向けたものであり、かつ目的受信者がその場にいて必要な秘密鍵を供給した場合に限り、このデータを使用して画像が生成される。

【００２０】本発明の他の態様は、目的画像出力機器へのデータの安全送信であって、このデータを使用して、目的受信者がいるときにだけ目的画像出力機器で画像を生成することができる送信に関する。この態様では、第１の鍵及び第２の鍵を使用してデータを２回にわたって暗号化する。第１の鍵は第１の秘密鍵／公開鍵対の公開鍵であり、第１の秘密鍵／公開鍵対の秘密鍵は本来、目的画像出力機器だけで所有され、第２の鍵は第２の秘密鍵／公開鍵対の公開鍵であり、第２の秘密鍵／公開鍵対の秘密鍵は本来、画像の目的受信者だけで所有される。次いで、２回暗号化データを目的画像出力機器に送信する。

【００２１】上記の構成によって、画像を生成するためのデータを画像出力装置に送信し、これによってこの画像を、目的受信者がいるときにだけ目的画像出力機器によって印刷することができる。

【００２２】他の態様では、本発明が、目的画像出力機器に送信された２回にわたって暗号化されたデータからの画像の生成であって、この２回にわたり暗号化された暗号化データを使用して、目的受信者がいるときにだけ目的画像出力機器で画像を生成することができる画像の生成を対象とする。この態様では、２回に亙り暗号化された暗号化データを受信し、次いで第１の鍵及び第２の鍵を使用して、この２回にわたり暗号化された暗号化データを２回にわたって復号する。第１の鍵は第１の秘密鍵／公開鍵対の秘密鍵であり、第１の秘密鍵／公開鍵対の秘密鍵は本来、画像の目的受信者だけによって所有される。第２の鍵は第２の秘密鍵／公開鍵対の秘密鍵であり、第２の秘密鍵／公開鍵対の秘密鍵は本来、目的画像出力機器だけによって所有される。次いで復号されたデータから画像を生成する。

【００２３】上記の構成によって、画像出力装置に送信されたデータがその画像出力装置に向けたものであり、かつ目的受信者がその場にいて必要な秘密鍵を供給した場合に限り、このデータを使用して画像が生成される。

【００２４】本発明の他の態様では、目的画像出力機器へのデータの安全送信方法であって、このデータを使用して、目的受信者がいるときに目的画像出力機器で画像を生成することができる方法が提供される。この方法は、第１の鍵を使用してデータを暗号化する第１の暗号化工程、ならびに第２の鍵及び第３の鍵を使用して第１の鍵を２回にわたって暗号化する第２の暗号化工程を含む。ここで第２の鍵は第１の秘密鍵／公開鍵対の公開鍵であり、第１の秘密鍵／公開鍵対の秘密鍵は本来、目的画像出力機器だけによって所有され、第３の鍵は第２の秘密鍵／公開鍵対の公開鍵であり、第２の秘密鍵／公開鍵対の秘密鍵は本来、画像の目的受信者だけによって所有される。次いで生成工程が、２回暗号化第１の鍵を含むヘッダを生成し、第１の送信工程ではヘッダを目的画像出力機器に送信する。受信工程では、暗号化データを要求するリクエストを目的画像出力機器から受信し、次いで第２の送信工程で、暗号化データを目的画像出力機器に送信する。

【００２５】上記の構成によって、印刷ジョブのヘッダを目的画像出力機器に送信することができるが、対応する暗号化データは、目的画像出力機器が必要とするまで目的画像出力機器に送信する必要はない。更に、データ

がその画像出力装置に向けたものであり、かつ目的受信者がその場にいて必要な秘密鍵を供給した場合に限り、目的画像出力機器を使用して画像が生成される。

【００２６】本発明の他の態様では、目的画像出力機器に送信されたデータから画像を生成する方法であって、このデータを使用して、目的受信者がいるときに目的画像出力機器で前記画像を生成することができる方法が提供される。この方法は、２回にわたって暗号化された第１の鍵を含むヘッダを受信する受信工程、及びヘッダに対応する暗号化されたデータを求める要求を送信する送信工程を含む。この方法は更に、ヘッダに対応する暗号化データを受信する受信工程、ならびに第２の鍵及び第３の鍵を使用して、２回にわたり暗号化された第１の鍵を２回にわたって復号する第１の復号工程を含む。第２の鍵は第１の秘密鍵／公開鍵対の秘密鍵であり、第１の秘密鍵／公開鍵対の秘密鍵は本来、前記画像の目的受信者だけによって所有され、第３の鍵は第２の秘密鍵／公開鍵対の秘密鍵であり、第２の秘密鍵／公開鍵対の秘密鍵は本来、目的画像出力機器だけによって所有される。こうして復号された第１の鍵を使用して暗号化データを復号する第２の復号工程が提供され、画像生成工程が復号されたデータから画像を生成する。

【００２７】上記の構成によって、印刷ジョブのヘッダを目的画像出力機器に送信することができるが、対応する暗号化データは、目的画像出力機器が必要とするまで目的画像出力機器に送信する必要はない。更に、データがその画像出力装置に向けたものであり、かつ目的受信者がその場にいて必要な秘密鍵を供給した場合に限り、目的画像出力機器を使用して画像が生成される。

【００２８】本発明は、方法又は装置、あるいはプリンタドライバなどのコンピュータ実行可能プロセス工程、安全印刷用のデータを送信するための画像出力装置、データを受信し印刷するプリンタ、ファクシミリ機などの専用装置として実施することができる。

【００２９】この短い要約は、本発明の本質を短時間に理解できるようにまとめたものである。本発明のより完全な理解は、本発明の好ましい実施形態の以下の詳細な説明を添付図面とともに参照することによって得ることができる。

【００３０】

【発明の実施の形態】本発明は一般に、目的受信者がいるときにだけ目的出力画像装置で画像データを印刷することができる画像データの安全印刷を対象とする。従って本発明は、ネットワーク化された環境にあるコンピュータから遠隔画像出力装置に文書を安全に送信することができる方法を提供する。文書は、目的受信者が目的画像出力機器のところに現れるまで安全に保持され、目的画像出力機器は目的受信者が現れた後にその画像を印刷する。

【００３１】図１に、本発明を実施することができるネットワーク化コンピューティング環境の全体システム図を示す。図１に示すとおりこのネットワーク化コンピューティング環境は、デスクトップコンピュータ１０、ラップトップコンピュータ２０、サーバ４０、ディジタル複写機３０及びプリンタ５０に接続されたネットワークを含む。ネットワーク１００は、バス型物理アーキテクチャから成るイーサネット（登録商標）・ネットワーク媒体であることが好ましい。ただし、インターネットを含むその他の種類のネットワーク上で本発明を利用することもできる。

【００３２】デスクトップコンピュータ１０は、Microsoft Windows95、Windows98、WindowsNTなどのウィンドウ操作環境を有するＩＢＭ　ＰＣ互換コンピュータであることが好ましい。一般的なＩＢＭ　ＰＣ互換コンピュータと同様に、デスクトップコンピュータ１０は、ディスプレイ、キーボード、マウス、フロッピィドライブ及び／又はその他の種類の記憶媒体（図示せず）を有することが好ましい。デスクトップコンピュータ１０には、更に、スマートカード１６などのコンピュータユーザのスマートカードとインターフェースするスマートカード・インターフェース装置１５が接続される。従って、スマートカード１６は、コンピュータユーザがデスクトップコンピュータ１０に対して本人であることを証明することができる機構を提供する。更に、このスマートカード１６は、コンピュータユーザ毎に固有で、後により詳しく説明するように、本発明において画像データの安全印刷に使用する秘密／公開鍵対の秘密鍵を含む。

【００３３】ラップトップコンピュータ２０も、Microsoft Windows95、Windows98、WindowsNTなどのウィンドウ操作環境を有するＩＢＭ　ＰＣ互換コンピュータである。デスクトップコンピュータ１０と同様に、ラップトップコンピュータ２０はディスプレイ、キーボード、マウス、及びフロッピィドライブ又はその他の記憶手段（図示せず）を有する。更に、ラップトップコンピュータ２０は、スマートカード２６などのコンピュータユーザのスマートカードにインターフェースする、その本体に接続されたスマートカード・インターフェース装置２５を有する。ネットワーク１００には更に、ネットワーク１００を介して印刷用の画像データを受け取ることができるディジタル複写機３０が接続されている。更に、ディジタル複写機３０には、スマートカード３６などの印刷ジョブ受信者のスマートカードとインターフェースするスマートカード・インターフェース装置３５が接続されている。更に、ネットワーク１００にはサーバ４０も接続されている。このサーバ４０は、DOS、Microsoft Windows95、Windows98、WindowsNT、ＵＮＩＸ（登録商標）などのオペレーティングシステムを有するＩＢＭ　ＰＣ互換コンピュータを含むことが好ましい。このサーバ４０は、多数のファイルを格納するための、好ましくは大容量固定ディスクである記憶装置４１を有する。従

って、ネットワーク１００上のその他の装置がサーバ４０をファイルサーバとして利用することができ、更にこのサーバ４０は、ネットワーク１００上のその他の装置に対しインターネットなどのその他のネットワークへのゲートウェイとして機能することができる。

【００３４】更に、プリンタ５０がネットワーク１００に接続されており、このプリンタ５０は、プリンタ及びファクシミリ装置として動作することができるレーザ又はバブルジェット（登録商標）（インクジェット）プリンタであることが好ましい。このプリンタ５０は、好ましくは大容量固定ディスクである記憶装置５１を有し、更に、プリンタ５０が受信したデータの暗号化及び／又は復号に使用するプリンタ５０に対応した秘密／公開鍵対の秘密鍵を含む埋込み型のスマートチップ５７を有する。更にプリンタ５０は、スマートカード５６などの印刷ジョブ受信者のスマートカードとインターフェースすることができるスマートカード・インターフェース装置５５に接続されている。これにより、スマートカード・インターフェース装置５５とスマートカード５６とをプリンタ５０内のスマートチップ５７と組み合わせて使用して、特定の目的受信者向けの印刷ジョブの印刷を制御することができる。

【００３５】図２は、デスクトップコンピュータ１０の内部アーキテクチャの概要を示すブロック図である。図２には、コンピュータバス２００にインターフェースされたプログラム可能マイクロプロセッサなどの中央処理装置（ＣＰＵ）２１０を含むデスクトップコンピュータ１０が示されている。コンピュータバス２００には更に、キーボードにインターフェースするキーボード・インターフェース２２０、ポインティングデバイスにインターフェースするマウス・インターフェース２３０、フロッピィディスクにインターフェースするフロッピィディスク・インターフェース２４０、ディスプレイにインターフェースするディスプレイ・インターフェース２５０、ネットワーク１００にインターフェースするネットワーク・インターフェース２６０、及びスマートカード・インターフェース装置１５にインターフェースするスマートカード・インターフェース２６５がそれぞれ結合されている。

【００３６】ランダム・アクセス・メモリ（ＲＡＭ）２７０がコンピュータバス２００にインターフェースして中央処理装置（ＣＰＵ）２１０にメモリ記憶域へのアクセスを提供し、これによってＣＰＵ２１０の実行時メインメモリとして機能する。具体的には、内蔵プログラム命令シーケンスを実行するときに、ＣＰＵ２１０は、これらの命令シーケンスを固定ディスク２８０（又は他のメモリ媒体）からランダムアクセスメモリ（ＲＡＭ）２７０にロードし、ＲＡＭ２７０からこれらの内蔵プログラム命令シーケンスを実行する。ウィンドウ機能オペレーティングシステムの下で使用可能な標準的なディスク・スワッピング手法によって、メモリ・セグメントをＲＡＭ２７０及び固定ディスク２８０へ、或いはそこからスワップすることができることにも留意されたい。リードオンリーメモリ（ＲＯＭ）２９０は、ＣＰＵ２１０に対するスタートアップ命令シーケンス、コンピュータ１０に接続された周辺装置の動作用の基本入出力オペレーション・システム（ＢＩＯＳ）などの不変命令シーケンスを格納する。

【００３７】固定ディスク２８０は、中央処理装置（ＣＰＵ）２１０が実行可能なプログラム命令シーケンスを格納して、オペレーティングシステム２８１、プリンタドライバ２８２、スマートカード・インターフェース・ドライバ２８３、その他のドライバ２８４、ワードプロセッシングプログラム２８５、その他のプログラム２８６、電子メールプログラム２８７及びその他のファイル２８８を構成する、コンピュータ可読媒体の一例である。前述のとおり、オペレーティングシステム２８１はウィンドウ機能オペレーティングシステムであることが好ましい。ただし本発明では、その他の種類のオペレーティングシステムを使用することもできる。プリンタドライバ２８２は、プリンタ５０などの少なくとも１台の画像出力装置で印刷する画像データを準備する目的に利用される。スマートカード・インターフェース・ドライバ２８３は、スマートカード１６などのスマートカードに読取り及び書込みを実行するために、スマートカード・インターフェース装置１５とインターフェースするスマートカード・インターフェース２６５を駆動及び制御する目的に利用される。その他のドライバ２８４には、コンピュータバス２００に結合された残りのそれぞれのインターフェースに対するドライバが含まれる。

【００３８】ワードプロセッシングプログラム２８５は、Microsoft Word, Corel WordPerfectなど、文書及び画像作成用の一般的なワードプロセッサプログラムである。その他のプログラム２８６には、デスクトップコンピュータ１０を動作させたり、所望のアプリケーションを実行させるのに必要なその他のプログラムが含まれる。電子メールプログラム２８７は、デスクトップコンピュータ１０がネットワーク１００を介して電子メールを送受信することを可能にする一般的な電子メールプログラムである。その他のファイル２８８には、デスクトップコンピュータ１０の動作に必要なファイル、又はデスクトップコンピュータ１０上のその他のアプリケーションプログラムが作成し、かつ／又は保持しているファイルが含まれる。

【００３９】図３は、プリンタ５０の内部アーキテクチャの概要を示すブロック図である。図３には、先に述べたようにプリンタ５０に対応する暗号化／復号目的の秘密鍵を含むプリンタスマートチップ５７を含むプリンタ５０が示されている。プリンタ５０は更に、プリンタバス３００にインターフェースされたプログラム可能マイ

クロプロセッサなどの中央処理装置（ＣＰＵ）３１０を含む。プリンタバス３００には更に、プリンタ５０のプリンタエンジン（図示せず）を制御する目的に利用される制御ロジック３２０、プリンタ５０のさまざまな入出力装置（図示せず）と通信する目的に使用されるＩ／Ｏポート３３０、スマートカード・インターフェース装置５５とインターフェースする目的に利用されるスマートカード・インターフェース３６５、及びプリンタ５０をネットワーク１００にインターフェースする目的に利用されるネットワーク・インターフェース３６０が結合されている。

【００４０】プリンタバス３００には更に、不揮発性プログラム命令を含むＥＥＰＲＯＭ３４０、ランダムアクセスメモリ（ＲＡＭ）３７０、プリンタメモリ５１及びリードオンリーメモリ（ＲＯＭ）３９０が結合されている。ＲＡＭ３７０は、プリンタバス３００にインターフェースしてＣＰＵ３１０にメモリ記憶域へのアクセスを提供し、これによってＣＰＵ３１０の実行時メインメモリとして機能する。具体的には、内蔵プログラム命令シーケンスを実行するときに、ＣＰＵ３１０は、これらの命令シーケンスをプリンタメモリ５１（又はその他のメモリ媒体）からＲＡＭ３７０にロードし、ＲＡＭ３７０からこれらの内蔵プログラム命令シーケンスを実行する。ＲＯＭ３９０は、ＣＰＵ３１０に対するスタートアップ命令シーケンス、プリンタ５０のさまざまな周辺装置（図示せず）の動作用のＢＩＯＳシーケンスなどの不変命令シーケンスを格納する。

【００４１】プリンタメモリ５１は、ＣＰＵ３１０が実行可能なプログラム命令シーケンスを格納して、プリンタエンジン・ロジック３５１、制御ロジックドライバ３５２、Ｉ／Ｏポートドライバ３５３、スマートカードインターフェース・ドライバ３５４、暗号化／復号ロジック３５５、待ち行列３５６、その他のファイル３５７、プリンタ・スマートチップ・ドライバ３５８及び電子メールプログラム３５９を構成する、コンピュータ可読媒体の一例である。プリンタエンジン・ロジック３５１及び制御ロジックドライバ３５２は、プリンタ５０が好ましくはネットワーク１００を介して受信した画像データに基づいて画像が印刷されるように、プリンタ５０のプリンタエンジン（図示せず）を制御及び駆動する目的に利用される。Ｉ／Ｏポートドライバ３５３は、Ｉ／Ｏポート３３０を介して接続された入出力装置（図示せず）を駆動する目的に利用される。スマートカード・インターフェース・ドライバ３５４は、スマートカード・インターフェース装置５５にインターフェースするスマートカード・インターフェース３６５を駆動する目的に利用され、これによって、プリンタ５０がスマートカード５６などのスマートカードに読取り及び書込みを実行することを可能にする。

【００４２】暗号化／復号ロジック３５５は、プリンタ５０が本発明に基づいて暗号化されたデータ（暗号化データ）を受信し、この暗号化印刷データを目的受信者がいるときに復号するのに必要な工程をプリンタ５０が実施することを可能にする。これらの工程の詳細については詳しく後述する。待ち行列３５６は、印刷する予定の多数の印刷ジョブから成る印刷待ち行列を含む目的に利用される。その他のファイル３５７には、プリンタ５０が動作するためのその他のファイル及び／又はプログラムが含まれる。プリンタ・スマートチップ・ドライバ３５８は、暗号化／復号目的でプリンタ・スマートチップ５７を駆動し、これとインターフェースする目的に利用される。最後に電子メールプログラム３５９は、プリンタ５０がネットワーク１００から電子メールメッセージを受信することを可能にする一般的な電子メールプログラムである。後に詳細に説明するように、このような電子メールメッセージに印刷ジョブ関連情報を含めることができる。

【００４３】図４は、サーバ４０の内部アーキテクチャの概要を示すブロック図である。図４には、コンピュータバス４００にインターフェースされたプログラム可能マイクロプロセッサなどの中央処理装置（ＣＰＵ）４１０を含むサーバ４０が示されている。コンピュータバス４００には更に、ネットワーク１００にインターフェースするネットワーク・インターフェース４６０が結合されている。更に、ランダムアクセスメモリ（ＲＡＭ）４７０、固定ディスク４１及びリードオンリーメモリ（ＲＯＭ）４９０もコンピュータバス４００に結合されている。ＲＡＭ４７０はコンピュータバス４００にインターフェースしてＣＰＵ４１０によるメモリ記憶域へのアクセスを提供し、これによってＣＰＵ４１０の実行時にメインメモリとして機能する。具体的には、内蔵プログラム命令シーケンスを実行するときに、ＣＰＵ４１０は、これらの命令シーケンスを固定ディスク４１（又はその他のメモリ媒体）からＲＡＭ４７０にロードし、ＲＡＭ４７０からこれらの内蔵プログラム命令シーケンスを実行する。標準的なディスクスワッピング手法によって、メモリセグメントをＲＡＭ４７０及び固定ディスク４１へ、ディスク４１からスワップすることができることも認識されたい。ＲＯＭ４９０は、ＣＰＵ４１０に対するスタートアップ命令シーケンス、サーバ４０（図示せず）に接続することができる周辺装置の動作用の基本入出力オペレーティングシステム（ＢＩＯＳ）などの不変命令シーケンスを格納する。

【００４４】固定ディスク４１は、ＣＰＵ４１０が実行可能なプログラム命令シーケンスを格納して、オペレーティングシステム４１１、ネットワーク・インターフェース・ドライバ４１２、暗号化／復号ロジック４１３、電子メールプログラム４１４、待ち行列４１５及びその他のファイル４１６を構成する、コンピュータ可読媒体の一例である。先に述べたとおりオペレーティングシス

テム４１１は例えば、DOS, Window95, Window98, WindowNT, UNIXなどのオペレーティングシステムである。ネットワークインターフェース・ドライバ４１２は、ネットワーク１００にサーバ４０をインターフェースするネットワーク・インターフェース４６０を駆動する目的に利用される。暗号化／復号ロジック４１３は、サーバ４０が暗号化データを受信し、このようなデータを待ち行列４１５中に保持したり、又は印刷のため、このようなデータをプリンタ５０などの画像出力装置に送ったりすることを可能にする。電子メールプログラム４１４は、一般的な電子メールプログラムであり、サーバ４０がネットワーク１００を介して電子メールメッセージを受信及び／又は送信することを可能にする。待ち行列４１５は、プリンタ５０などの１台又は数台の画像出力装置に出力する多数の印刷ジョブを格納する目的に利用される。最後にその他のファイル４１６には、サーバ４０を動作させ、かつ／又はサーバ４０に追加機能を提供するのに必要なその他のファイル又はプログラムが含まれる。

【００４５】図５Ａは、デスクトップコンピュータ１０などのネットワーク１００上のコンピュータのコンピュータ・ユーザが、印刷ジョブに関係したデータを送信し、目的受信者がいるときにだけ目的画像出力機器で印刷することができる本発明の暗号化プロセスを説明するための図である。例えば、デスクトップコンピュータ１０の前にいるコンピュータユーザが、ワードプロセッシングプログラム２８５を使用して文書を作成し、その文書を、目的受信者が、プリンタ５０の場所に居るときに限ってプリンタ５０で印刷したいことがある。最も重要なのは、プリンタ５０以外の装置又は目的受信者以外の人物によってこの印刷ジョブがアクセスされたり、又は閲覧されたりしないようにしたいと、このデスクトップコンピュータ１０の前にいるコンピュータユーザが思っていることである。

【００４６】従って本発明は、画像データを暗号化して、他のコンピュータ・ユーザ又はネットワーク１００上の装置がアクセスできないようし、また、目的受信者が目的のプリンタ（目的プリンタ）のところに物理的に現れるまで、画像データが暗号化されたままの状態に維持されるようにする。こうすれば、目的プリンタ５０で印刷する前の時点で暗号化データがアクセスされた場合でもあっても、データは理解不能なビットの羅列としてしか現れない。

【００４７】具体的には、この暗号化プロセスは、図５Ａに示すように画像データ５０１から開始される。画像データ５０１は、デスクトップコンピュータ１０の前にいるコンピュータユーザによってワードプロセッシングプログラム２８５などのプログラムを使用して作成されることが好ましい。画像データ５０１に対応する印刷ジョブを目的受信者に受信してもらうために、プリンタ５０などの目的プリンタに送信する準備が整うと、ユーザは、ワードプロセッシングプログラム２８５中に提供されたボタンを押して、この文書が安全印刷によって印刷すべき文書であることを指示することが好ましい。

【００４８】この好ましい形態では、プリンタドライバ２８２がこの暗号化プロセスを処理してデータ５０１を暗号化した後に、これをネットワーク１００を介してプリンタ５０に送信する。プリンタドライバ２８２が、対称暗号化アルゴリズムとともに使用するランダムに生成された対称鍵を生成することが好ましい。次いでデータ５０１を、ランダムに生成された対称鍵５１０を使用し対称暗号化アルゴリズムを適用することによって暗号化し、これによって対称に暗号化されたデータ（対称暗号化データ）５０２を作成する。これにより、この対称暗号化データ５０２は、同様の対称暗号化アルゴリズム及び対称鍵５１０のコピーを有する装置でしか復号できなくなる。従って、このデータを最終的に復号し目的受信者に対して印刷するためには、対称鍵５１０及び対称暗号化データ５０２をプリンタ５０に渡さなければならない。データ５０１をプリンタ５０で印刷するときまでセキュリティを維持するため、対称鍵５１０も、目的プリンタと目的受信者とに対応する２つの公開鍵を用いて暗号化する。それぞれの公開鍵は、非対称暗号化アルゴリズムで使用される公開鍵／秘密鍵対に由来する。こうすると目的受信者の秘密鍵と目的プリンタの秘密鍵を組み合わせない限り対称鍵５１０を復号することはできず、そのため対称暗号化データ５０２を復号して印刷することもできない。

【００４９】従って図５Ａに示すように、プリンタ５０に対応するプリンタ公開鍵５２０を、ネットワーク１００上のサーバに搭載された公開鍵インフラストラクチャから、又はネットワーク１００を介して第三者鍵サービスから、又はローカル鍵格納ファイルなどの適当なその他の供給元から入手する。次いでプリンタ公開鍵５２０を非対称暗号化アルゴリズムとともに利用して対称鍵５１０を暗号化し、これによってプリンタ鍵で暗号化された対称鍵（プリンタ鍵暗号化対称鍵）５１１を作成する。こうすると、プリンタ５０に対応する公開／秘密鍵対の対応する秘密鍵がないと対称鍵５１０にはアクセスできない。前述したように、プリンタ５０の秘密鍵は、他の人物又は装置に対して露出することがないように、プリンタ５０の内部に埋め込まれたスマートチップ５７の中に保持されることが好ましい。こうするとプリンタ鍵暗号化対称鍵５１１は、目的画像出力機器、このケースではプリンタ５０でしか復号することができない。

【００５０】以上の対称鍵５１０の暗号化は、目的プリンタだけが印刷ジョブを印刷できることを保証するが、目的受信者だけが印刷ジョブを受け取り、それを見るということを保証するものではない。従って、目的受信者に対応する公開鍵を用いて対称鍵５１０を更に暗号化す

ることが好ましい。図５Ａに示すように受信者公開鍵５３０を、公開鍵インフラストラクチャ又はその他の適当な供給元から得る。次いで、受信者公開鍵５３０を非対称暗号化アルゴリズムとともに使用してプリンタ鍵暗号化対称鍵５１１を再び暗号化し、２回にわたって暗号化した対称鍵（２回暗号化対称鍵）５１２を作成する。この２回にわたり暗号化された対称鍵５１２は、第１層がプリンタ公開鍵５２０で、第２層が受信者公開鍵５３０で暗号化されて図示されており、これによって目的受信者の秘密鍵と目的プリンタの秘密鍵の特定の組合せが提示されない限り対称鍵５１０へのアクセスが防止されることになる。

【００５１】図５Ａに更に示すように、２回にわたり暗号化された対称鍵５１２を含み、更に送信者の識別、目的受信者の識別、印刷ジョブのサイズ、プリンタに関係した照合オプション、選別オプション、用紙選択オプションの設定などの印刷ジョブに関係した情報を含むヘッダ５５１が提供される。こうすると、最終的な印刷のための印刷ジョブの待ち行列化及び印刷ジョブの識別を目的とした印刷ジョブ自体に関係する非機密情報を、目的プリンタに提供することができる。ヘッダ５５１がその他の種類の情報を含むことができること、及びヘッダ５５１を、２回にわたり暗号化された対称鍵５１２を含まないフォーマットで提供することもできることを理解されたい。

【００５２】この好ましい実施の形態では、ヘッダ情報５４０が２回にわたり暗号化された対称鍵５１２にプリペンドされてヘッダ５５１が生成される。ヘッダ５５１を作成した後、ヘッダ５５１及び対称暗号化データ５０２がどんな形であれ変更されていないことを受信側装置が検証することができる完全性チェックを可能にするため、ヘッダ５５１及び対称暗号化データ５０２に完全性アルゴリズムを適用する。具体的には、データの完全性を保証する目的に使用されるハッシュアルゴリズム５７０を用いてヘッダ５５１及び対称暗号化データ５０２を処理する。このアルゴリズムの結果、対応するデータに対する一種のチェックサムを表す「ハッシュ」として知られる値が得られる。

【００５３】従って、データハッシュ５５３及びヘッダハッシュ５５４が作成され、これらはその後、印刷ジョブを開始した送信者に対応する秘密鍵／公開鍵対の送信者秘密鍵５６０を使用してディジタル署名される。このようにしてヘッダ５５１、対称暗号化データ５０２、データハッシュ５５３及びヘッダハッシュ５５４を含む印刷ジョブ５５０が作成される。送信者秘密鍵５６０は、デスクトップコンピュータ１０の前にいる送信者が所有するスマートカード１６などのスマートカードからスマートカード・インターフェース装置１５を介して得ることが好ましい。送信者と目的受信者が同一である場合には、送信者秘密鍵５６０は、受信者公開鍵５３０と同じ秘密鍵／公開鍵対に由来する。このような状況では、送信者は遠隔地から目的プリンタに安全印刷ジョブを送信することができ、後に自身のスマートカードを用いて目的プリンタのところで印刷ジョブを取り出すことができる。

【００５４】こうすると、目的画像出力機器、このケースではプリンタ５０に印刷ジョブ５５０を送信して、待ち行列に入れ、目的受信者がいるときに最終的に印刷することができる。目的プリンタ５０は次いで、印刷ジョブ５５０の送信者の認証、印刷ジョブ５５０のヘッダ５５１及び暗号化データ５０２の完全性の検証、２回にわたり暗号化された対称鍵５１２の復号、最後に、プリンタ５０で印刷するための暗号化データ５０２の復号を実行することができる。

【００５５】図５Ａに示した暗号化構成が本発明の好ましい一実施の形態であるが、安全印刷ジョブに対応するデータをその他の組合せの公開鍵を使用して暗号化すること、及び前述の公開鍵を使用し非対称暗号化アルゴリズムを用いてデータを直接に暗号化することができることを理解されたい。例えば、対称鍵５１０の暗号化の順序を逆にすること、すなわち、まず受信者公開鍵５３０を使用して対称鍵５１０を暗号化し、次いでプリンタ公開鍵５２０を使用して暗号化することができる。従って２回暗号化対称鍵５１２は、まず目的プリンタの秘密鍵を使用して復号され、次いで目的受信者の秘密鍵を使用して復号されることになる。

【００５６】図５Ｂでは、図５Ａに示した対称鍵を用いる代わりに目的プリンタ及び目的受信者の公開鍵を非対称暗号化アルゴリズムとともに使用して、安全印刷ジョブに関連したデータを２回にわたって暗号化する。図５Ｂでデータ５８１は安全印刷ジョブに関連した印刷データである。図５Ａの場合と同様に、まず目的プリンタの公開鍵（５２０）及び目的受信者の公開鍵（５３０）を公開鍵インフラストラクチャ又はその他の適当な供給元から入手する。その後、受信者公開鍵５３０とともに非対称暗号化アルゴリズムを使用してデータ５８１を暗号化し、受信者鍵で暗号化されたデータ（受信者鍵暗号化データ）５８２を作成する。次いでプリンタ公開鍵５２０とともに非対称暗号化アルゴリズムを使用して受信者鍵暗号化データ５８２を再び暗号化し、２回にわたる暗号化データ５８３を作成する。従って図５Ｂに示すとおり、目的プリンタへの送信のためにデータ自体が２回にわたって暗号化され、それ以降は、目的プリンタの秘密鍵と目的受信者の秘密鍵がなければデータを復号することができない。

【００５７】このように、図５Ｂに示した暗号化構成を利用して、図５Ａに示した対称鍵を使用せずに文書の安全印刷を普通に実施することができる。図５Ｂの構成を、２回に亙り暗号化した暗号化データを目的プリンタへ送信する前にヘッダ及び署名されたハッシュ（署名付

きハッシュ）を作成するなどの図５Ａのその他の特徴と組み合わせることもできる。図５Ｂに示すデータ５８１に対応する潜在的に大きなデータの２重暗号化では、対称鍵５１０だけを２重暗号化する図５Ａの暗号化構成よりもはるかに多くのコンピューティング資源が必要となる可能性があるため、図５Ａの暗号化構成のほうがより好ましい実施形態であることに留意されたい。

【００５８】図５Ｃは、図５Ａに基づいて暗号化したデータ５０１の復号及び印刷を説明するための図である。まず印刷ジョブ５５０が、ネットワーク１００を介して目的プリンタ、このケースではプリンタ５０で受信される。印刷ジョブ５５０は、図５Ａに示したものと同じ構成要素を含む。次に送信者公開鍵５６１を、好ましくは公開鍵インフラストラクチャ又はその他の適当な供給元から入手する。送信者公開鍵５６１は、デスクトップコンピュータ１０の前にいるこの印刷ジョブをプリンタ５０に送ったコンピュータユーザに対応する。代替として送信者公開鍵５６１を、ヘッダ情報５４０の中に含まれる送信者のディジタル証明書のコピー中に含めてもよい。次いで送信者公開鍵５６１をハッシングアルゴリズム５７０とともに使用して、ヘッダ５５１及び対称暗号化データ５０２の完全性を認証及び検証する。具体的には、署名付きヘッダハッシュ５５４及び署名付きデータハッシュ５５３を送信者公開鍵５６１を使用して認証して、印刷ジョブ５５０の作成者が確かにその送信者であることを検証する。この認証が失敗に終わった場合にはその印刷ジョブを廃棄することが好ましい。

【００５９】次に、印刷ジョブ５５０をプリンタ５０の待ち行列３５６に入れるか、又は代替としてサーバ４０の待ち行列４１５に入れ、プリンタ５０による後のアクセスに備える。プリンタ５０のところに目的受信者が物理的に現れると、スマートカード５６などの受信者のスマートカードがスマートカード・インターフェース装置５５に挿入されることによって受信者秘密鍵５３１が得られる。セキュリティの理由から、受信者秘密鍵５３１はスマートカード５６上にだけ保持され、プリンタ５０はこれを読むことができない。従って、２回にわたり暗号化された対称鍵５１２は、スマートカード・インターフェース装置５５を介してプリンタ５０からスマートカード５６に渡され、そこで受信者秘密鍵５３１を使用して部分的に復号される。その後、この部分的に復号された対称鍵５１１をスマートカード５６からプリンタ５０に戻し、プリンタ５０のスマートなチップ５７の内部で完全に復号する。その結果、「クリア・テキスト」の形態の対称鍵５１０が得られる。

【００６０】次いで、対称鍵５１０を利用して対称暗号化データ５０２を復号し、クリアテキストの形態のデータ５０１を得る。次いで、この復号されたデータ５０１に基づいて画像をプリンタ５０上で印刷する。このようにして本発明が、目的プリンタに文書又は画像を送信して目的受信者がいるときにだけ印刷する能力を提供することが理解される。目的プリンタが置かれている場所に目的受信者がいることが検証されるまで印刷ジョブは暗号化された形態のまま維持され、この暗号化データを傍受した人物又は装置がこれを合理的に復号することはできない。

【００６１】図５Ｄは、図５Ｂに示した代替形態に従って暗号化した２回暗号化印刷データ５８３の復号及び印刷を説明するための図である。まず２回にわたり暗号化された暗号化データ５８３が、スマートカード・インターフェース５５を介して目的受信者のスマートカード５６に渡され、次いで、スマートカード５６の中にある受信者秘密鍵５３１を使用して部分的に復号される。次いでスマートカード５６は、部分的に復号された新たなデータ５８２をプリンタ５０の制御に戻す。部分的に復号されたデータ５８２は次にプリンタ５０のスマートチップ５７に渡され、そこで、プリンタ５０内のスマートチップ５７に含まれるプリンタ秘密鍵５２１を使用して完全に復号される。復号された「クリア」データ５８１は次に、スマートチップ５７からプリンタ５０に戻され印刷される。

【００６２】図５Ｂ及び５Ｄに記載した暗号化／復号は目的受信者に対する目的プリンタへの安全印刷を提供するが、２回に亙り暗号化された暗号化データを処理するのにはスマートチップ５７及びスマートカード５６が、図５Ａ及び５Ｃに示した２回にわたり暗号化された対称鍵の処理に比べ、はるかに多くの資源を必要とする可能性がある。図５Ｄの復号プロセスには、図５Ｂに示した認証、完全性の検証などのその他の付随的な特徴を組み込むこともできる。

【００６３】図５Ａに示したハッシングプロセスは、プリンタ５０などの受信側装置が対称暗号化データ５０２の完全性を検証することを可能にする一種のチェックサムである署名付きデータハッシュ５５３を提供する。

【００６４】図６に、データに対する署名付きハッシュを生成しフォーマットする１つの方法を説明するための図を示す。図６は、安全に印刷すべき画像に対応する印刷データ６０１が非暗号化「プレーンテキスト」フォーマットを示す。次いで、一方向ハッシュ関数であることが好ましいハッシングアルゴリズムを印刷データ６０１に適用して、実質上のメッセージ・ダイジェストであるデータハッシュ６１０を作成する。次いで、図５Ａの送信者秘密鍵５６０などの送信者の秘密鍵を使用してデータハッシュ６１０にディジタル署名する。この署名したハッシュ６１１を任意選択で暗号化してもよい。いずれの場合も、署名付きハッシュ６１１は、目的プリンタに送信するデータブロック６００の一部である署名付きハッシュ６１２にコピーされ、目的プリンタで認証及び完全性検証目的に使用される。

【００６５】図７Ａは、本発明の好ましい実施の形態に

基づくヘッダの構造を説明するための図である。具体的には、まず最初に受信者ＩＤ７０１、送信者ＩＤ７０２及び対称鍵７０３がクリアなプレーンテキストフォーマット（クリアプレーンテキスト・フォーマット）で提供され、図７Ａに示すヘッダ７００に包含される。受信者ＩＤ７０１、送信者ＩＤ７０２及び対称鍵７０３に対してこれらをひとまとまりとしてハッシングアルゴリズムを実行し、ハッシュ７２０を作成する。次いで、図５Ａに示した送信者秘密鍵５６０などの送信者の秘密鍵を用いてハッシュ７２０に署名して、署名付きハッシュ７２１を作成する。次いで、署名付きハッシュ７２１を任意選択で暗号化してもよい。いずれの場合も署名付きハッシュ７２１は署名付きハッシュ７２２にコピーされ、ヘッダ７００に包含される。

【００６６】受信者ＩＤ７０１は、クリア・プレーンテキストフォーマットのまま受信者ＩＤ７１１にコピーされ、ヘッダ７００に包含される。代替として、目的受信者を匿名にするために目的プリンタの公開鍵を用いて受信者ＩＤ７０１を暗号化し、受信者ＩＤ７１１にコピーし、ヘッダ７００に包含してもよい。いずれの場合も、目的プリンタは、ヘッダを受け取った後に受信者ＩＤ７１１を抽出して読むことができ、これによって目的受信者に対応する印刷ジョブを待ち行列に入れることができる。ヘッダ７００に含める前に目的プリンタの公開鍵を用いて送信者ＩＤ７０２を暗号化してもよい。但し、このような暗号化は必要ない。いずれにしても送信者ＩＤ７０２は送信者ＩＤ７１２にコピーされ、ヘッダ７００に包含される。対称鍵７０３は図５Ａに示したように２回暗号化し、次いで２回暗号化対称鍵７１３としてヘッダ７００に包含することが好ましい。

【００６７】暗号化データとは別に目的プリンタに送信することができるように構築されたヘッダの代替構造を図７Ｂに示す。具体的には、最初に受信者ＩＤ７５１、送信者ＩＤ７５２、対称鍵７５３及びユニフォーム・リソース・ロケータ（ＵＲＬ）７５４がクリアプレーンテキスト・フォーマットで提供され、図７Ｂに示すヘッダ７５０に包含される。ＵＲＬ７５４は、後に取り出して目的プリンタに送信する目的で暗号化データが格納されたアドレスの場所であることが好ましい。例えば、図５Ａに示した２回暗号化データ５１２が、デスクトップコンピュータ１０の固定ディスク２８０又はサーバ４０の固定ディスク４１上のＵＲＬ７５４に対応する記憶場所に保持されているとする。次いでＵＲＬ７５４はヘッダ７５０に包含され、ヘッダ７５０は、対応する暗号化データなしで目的プリンタに送信される。続いて、ＵＲＬ７５４への参照を含むリクエストを目的プリンタから受け取ると、デスクトップコンピュータ１０又はサーバ４０は、対応する暗号化データを目的プリンタに送る。こうすると、目的プリンタは、暗号化データを格納するためのメモリ空間をデータが必要となるまで使用せず、必要となったときに、対応するＵＲＬ７５４を参照することによって暗号化データをその記憶場所から引き出す。

【００６８】受信者ＩＤ７５１、送信者ＩＤ７５２、対称鍵７５３及びＵＲＬ７５４に対してこれらを一纏まりとしてハッシングアルゴリズムを実行し、ハッシュ７７０を作成する。次いで、図５Ａに示した送信者秘密鍵５６０などの送信者の秘密鍵を用いてハッシュ７７０に署名し、署名付きハッシュ７７１を作成する。セキュリティを更に高めるために任意選択で署名付きハッシュ７７１を暗号化してもよい。いずれの場合も署名付きハッシュ７７１は署名付きハッシュ７７２にコピーされ、ヘッダ７５０に包含される。

【００６９】受信者ＩＤ７５１は、クリアプレーンテキスト・フォーマットのまま受信者ＩＤ７６１にコピーされ、ヘッダ７５０に包含される。代替として、目的受信者を匿名にするために目的プリンタの公開鍵を用いて受信者ＩＤ７５１を暗号化し、受信者ＩＤ７６１にコピーし、ヘッダ７５０に包含してもよい。いずれの場合も、目的プリンタはヘッダを受け取った後に受信者ＩＤ７６１を抽出して読むことができ、これによって目的受信者に対応する印刷ジョブを待ち行列に入れることができる。ヘッダ７５０に含める前に目的プリンタの公開鍵を用いて送信者ＩＤ７５２を暗号化してもよい。但し、このような暗号化は必要ない。いずれにしても送信者ＩＤ７５２は送信者ＩＤ７６２にコピーされ、ヘッダ７５０に包含される。対称鍵７５３は図５Ａに示した方法に従って２回に亙り暗号化され、次いで２回にわたり暗号化された対称鍵７６３としてヘッダ７５０に包含することが好ましい。この代替ヘッダフォーマットでは、ＵＲＬ７５４も、目的プリンタの公開鍵又は対称鍵７５３を用いて暗号化され、次いでヘッダ７５０のＵＲＬ７６４に格納される。

【００７０】この構成によって、ヘッダ７５０に対応する暗号化データを送信する前に、ヘッダ７５０を別個に目的プリンタに送信することができる。本発明のこの実施形態では、デスクトップコンピュータ１０の電子メールプログラム２８７を通じてヘッダ７５０が電子メールメッセージを介してプリンタ５０などの目的プリンタに送信され、プリンタ５０の電子メールプログラム３５９によって受信されることが好ましい。１つ又は複数のネットワークプロトコルを使用するなど、ネットワーク１００を介してヘッダ７５０をプリンタ５０に送信するその他の手段を使用することもできる。目的受信者がプリンタ５０のところに現れたときなど暗号化データが必要となったとき、プリンタ５０はＵＲＬ７５４を復号し、ＵＲＬ７５４への参照を含むデータ・リクエストを送信することができる。次いでＵＲＬ７５４に対応する暗号化データが復号及び印刷のために目的プリンタに送られる。次いで好ましくは図５Ｃに記載した方法で対称鍵７６３が復号され、その後、目的受信者がいるときに暗号

化データが復号され印刷される。こうすると、復号及び印刷のために印刷データを取り出す必要が生じるまでは、目的プリンタのメモリ容量又は目的プリンタが利用するファイルサーバのメモリ容量に、大きな暗号化印刷データファイルを格納する負担がかからない。

【００７１】図８は、本発明の好ましい実施形態に基づく安全印刷ジョブの暗号化及び送信を全般的に説明するための流れ図である。この図に示すプロセス工程ならびに図９のプロセス工程は、ディスク２８０、ディスク４１、プリンタメモリ５１などのコンピュータ可読メモリ媒体上に格納されたコンピュータ実行可能プロセス工程である。まずステップＳ８０１で、ネットワーク化されたコンピューティング環境にあるコンピュータで作業している送信者が、目的受信者がいるときにプリンタ又はファクシミリ装置などの目的画像出力機器で安全印刷する文書又は画像を送信する印刷ジョブを実行依頼する。この印刷ジョブが、Microsoft Wordなどのワードプロセッシングアプリケーション中のボタンを押すことによって実行依頼され、その後、プリンタドライバインターフェースが現れて目的受信者などの必要な情報を集めることが好ましい。代替として、このような情報を集めるために別個のクライアント・アプリケーションを提供してもよい。プリンタドライバが、安全印刷ジョブの暗号化及び送信のための図８の残りのステップも実行することが好ましい。

【００７２】次に、図５Ａに関して前述したように、この印刷ジョブに関連した画像データを、ランダムに生成された対称鍵を対称暗号化アルゴリズムとともに用いて暗号化する（ステップＳ８０２）。次にステップＳ８０３で、目的受信者の公開鍵及び目的プリンタの公開鍵を公開鍵インフラストラクチャ又はその他の適当な供給元から入手し、送信者の秘密鍵を、好ましくは送信者が所有するスマートカード１６からスマートカード・インターフェース装置１５を介して入手する。次にステップＳ８０４で、まず目的プリンタの公開鍵を非対称暗号化アルゴリズムとともに用いて対称鍵を暗号化し、次いで目的受信者の公開鍵を非対称暗号化アルゴリズムとともに用いて対称鍵を再び暗号化することにより、対称鍵を２回にわたって暗号化する。

【００７３】こうして対称鍵を２回にわたり暗号化した後、この２回暗号化された対称鍵を含み、更に目的受信者及び送信者の識別などの印刷ジョブに関係した情報を非暗号化フォーマットで含むヘッダを形成する（ステップＳ８０５）。このヘッダが暗号化データとは別に送られる場合には、前述したように、ヘッダが更に、ヘッダに対応する暗号化データの記憶場所を指すＵＲＬを含むことができる。次いでステップＳ８０６に進み、ハッシングアルゴリズムをヘッダに適用してヘッダハッシュを形成し、暗号化データに適用してデータハッシュを形成する。次いでステップＳ８０７に進み、送信者の秘密鍵を用いてヘッダハッシュ及びデータハッシュにディジタル署名する。追加のセキュリティのために任意選択で、ヘッダハッシュ及びデータハッシュを暗号化してもよい。送信者の秘密鍵は、送信者が所有するスマートカードから得ることが好ましい。代替として、送信者の秘密鍵を安全に格納する目的にトークン、フラッシュＲＯＭ又はその他の記憶手段を使用することもできる。

【００７４】次にステップＳ８０８に進み、ヘッダを、対応する暗号化データとは別に目的プリンタに送るかどうかを判定する。ヘッダを別個に送る場合には制御がステップＳ８０９に移り、ヘッダ及びヘッダハッシュを含む印刷ジョブを、対応する暗号化データを付けずにネットワークを介して目的プリンタへ送信する。目的プリンタが電子メールプログラムを有し、ヘッダ及びヘッダハッシュを含む印刷ジョブが電子メールによってプリンタへ送られることが好ましい。但し、１つ又は複数のその他のネットワーク・プロトコルを経由するなど、その他の手段によって印刷ジョブを別個に目的プリンタへ送ることもできる。この好ましい態様では、ヘッダが、暗号化データ及びデータハッシュの記憶場所に対応するＵＲＬを含む。この記憶場所は、ネットワークを介して目的プリンタがアクセスすることができるコンピュータ又はサーバのディスク上に置くことができる。次いで対応する暗号化データ及びデータハッシュが、ステップＳ８１０で暗号化データ及びデータハッシュが格納されたサーバ又はコンピュータによって、自動的に又は目的プリンタのリクエストに応答して先に受信されたヘッダに入れて目的プリンタに渡されたＵＲＬを参照することによって目的プリンタに送られる。次いで制御は終了（ステップＳ８１２）に至る。

【００７５】しかしステップＳ８０８で、ヘッダを対応する暗号化データと一緒に目的プリンタに送ると判定された場合には、制御はステップＳ８１１に移り、ヘッダ、ヘッダハッシュ、暗号化データ及びデータハッシュを含む印刷ジョブをネットワークを介して目的プリンタに送信する。次いで制御はステップＳ８１２に至り終了となる。この実施形態では目的プリンタが、暗号化データを復号するための２回暗号化対称鍵を含むヘッダと一緒に暗号化データを受け取る。更に目的プリンタは、ヘッダ及び暗号化データの正当性及び完全性を検証するためのヘッダハッシュ及びデータハッシュを受け取る。

【００７６】図９は、本発明の好ましい実施形態に基づく安全印刷ジョブの復号及び印刷を説明するための流れ図である。まずステップＳ９０１で目的プリンタが安全印刷ジョブを受け取る。図８に関して前述したように、ヘッダ及びヘッダハッシュを目的プリンタが電子メールで別に受け取る場合には、印刷ジョブがヘッダ及びヘッダハッシュだけを含む。そうでない場合には、印刷ジョブがヘッダ及びヘッダハッシュとともに暗号化データ及びデータハッシュを含み、ネットワークを介した通常の

手段によって目的プリンタで受信される。

【００７７】次に、後段の安全印刷ジョブの完全性の認証及び検証に使用する送信者の公開鍵を、公開鍵インフラストラクチャ、他の適当な供給元、又はヘッダの中に提供された送信者のディジタル証明書のコピーから得る（ステップＳ９０２）。次にステップＳ９０３で、送信者の公開鍵を使用して、安全印刷ジョブのヘッダハッシュのディジタル署名の正当性をチェックする。ヘッダハッシュが本物でない場合、制御はステップＳ９０４に移り、認証されなかった印刷ジョブが検出されたことを送信者に警告する通知を送信者に送ることが好ましい。次にステップＳ９０５でこの印刷ジョブを廃棄する。フローは次いでステップＳ９１９に至り終了となる。しかしステップＳ９０３でヘッダハッシュが本物であると判定された場合、フローはステップＳ９０６に進み、ヘッダの完全性をヘッダハッシュに照らして検証する。

【００７８】次にステップＳ９０６で、ハッシングアルゴリズムを使用してヘッダをヘッダハッシュと比較し、ヘッダが損なわれることなく受信され、不正に操作されておらず、従って信頼できる完全性を有するものであることを指示するかどうかを検証する。ヘッダの完全性に問題がある場合には制御はステップＳ９０５に移り、この印刷ジョブを廃棄する。次いで制御はステップＳ９１９に至り終了となる。しかし、ヘッダが信頼できる完全性を有する場合には制御はステップＳ９０７に進み、目的受信者の識別などのヘッダ情報をヘッダから抽出し、その後、後段の印刷のために印刷ジョブを印刷待ち行列に入れる。印刷ジョブはプリンタからネットワーク上のローカル・サーバに送り、そこで、目的プリンタが後に取り出すまで目的受信者の識別に基づいて印刷待ち行列に入れておくことが好ましい。代替としてこの印刷待ち行列を、目的プリンタ自体の大容量記憶装置内に維持してもよい。

【００７９】ステップＳ９０８では、目的受信者が目的プリンタのところに到着し、目的プリンタに接続されたスマートカード・インターフェース装置に自身が所有するスマートカードを挿入する。スマートカードが固有の秘密鍵を含み、更に目的受信者に対応する認証識別情報を含むことが好ましい。プリンタは、スマートカード・インターフェース装置を介してスマートカードから目的受信者の認証識別情報を入手し、目的受信者の識別が本物かどうかを判定する（ステップＳ９０９）。ここで識別情報が本物でない場合、制御はステップＳ９１９に至り終了となる。識別情報が本物である場合には、プリンタ自体又はローカル・サーバに位置する印刷待ち行列に、好ましくは目的受信者の識別への参照によって問い合わせ、目的受信者に対応する印刷ジョブがあるかどうかを判定する（ステップＳ９１０）。印刷待ち行列中に目的受信者に対応する印刷ジョブがない場合には、制御はステップＳ９１９に至り終了となる。一方、印刷待ち行列中に目的受信者に対応する印刷ジョブがある場合には印刷待ち行列中の次順の印刷ジョブを入手し、制御はステップＳ９１１に移る。

【００８０】ステップＳ９１１では印刷ジョブを調べ、暗号化データ及びデータハッシュを付けずにヘッダ及びヘッダハッシュだけが電子メールによって別個にプリンタに送信された場合のように、印刷ジョブがヘッダ及びヘッダハッシュだけを含むものであるかどうかを判定する。そうである場合には、目的プリンタが、暗号化データを取り出すよう求めるリクエストをネットワーク上のサーバ又はコンピュータなどの暗号化データが格納された場所に送り、その後、暗号化データ及び対応するデータハッシュが、このサーバ又はコンピュータから目的プリンタに送信される（ステップＳ９１２）。この好ましい態様では、暗号化データを取り出すよう求める目的プリンタへの要求が、目的プリンタが以前に受け取ったヘッダに含まれるＵＲＬへの参照を含む。このＵＲＬは、暗号化データ及び対応するデータハッシュの記憶場所を指す。こうすれば、印刷のため必要になるまで目的プリンタが大きな暗号化データファイルを格納する必要がなく、暗号化データは、必要となったときにサーバ又はコンピュータ上の記憶場所から目的プリンタに引き出される。プリンタによる取出しリクエスト及びこれに続く暗号化データ及びデータハッシュの送信は、取出しリクエストがＵＲＬへの参照を含むＴＣＰ／ＩＰプロトコル、ＨＴＴＰプロトコルなどの通常のネットワーク通信手段によって実施されることが好ましい。ただし、ＦＴＰなどのその他のプロトコルを使用することもできる。制御は次いでステップＳ９１３に移る。ヘッダが別個に目的プリンタに送られたのではないとステップＳ９１１で判定された場合には、印刷ジョブがヘッダとともに暗号化データを既に含んでおり、従って制御は直接にステップＳ９１３に移る。

【００８１】次にステップＳ９１３で、印刷ジョブのヘッダから２回にわたり暗号化した対称鍵を抽出し、目的受信者の秘密鍵を非対称復号アルゴリズムとともに使用して部分的に復号する。この好ましい実施の形態では、目的受信者のスマートカードが目的受信者の秘密鍵を含み、更にマイクロプロセッサを含む。そのため２回にわたり暗号化された対称鍵は、スマートカード・インターフェース装置を介して目的プリンタからスマートカードに渡される。こうすると、この部分的復号がスマートカード上で実際に実施され、これによってスマートカード上に含まれる目的受信者の秘密鍵への外部アクセスが防止される。

【００８２】次いで、部分的に復号された対称鍵がスマートカードからプリンタに戻され、その後、目的プリンタの秘密鍵を非対称復号アルゴリズムとともに使用して、この部分的に復号された対称鍵を完全に復号する（ステップＳ９１４）。目的プリンタの秘密鍵は、プリ

ンタの内部に埋め込まれたスマートチップの中に含まれることが好ましい。部分的に復号された対称鍵はスマートチップに渡され、そこでスマートチップに含まれる秘密鍵を使用して完全に復号され、これによって、スマートチップ上に含まれるプリンタの秘密鍵への外部アクセスが防止される。トークン、フラッシュＲＯＭなど、目的プリンタの秘密鍵を格納するその他の手段を使用することもできる。

【００８３】次いで、完全に復号された「クリア」な対称鍵をスマートチップから目的プリンタに戻し、その後、この復号された「クリア」な対称鍵を使用して、暗号化データを対称復号アルゴリズムに従って復号する（ステップＳ９１５）。次にステップＳ９１６に進み、復号されたデータの完全性を、前述したように、ハッシングアルゴリズムを使用してこのデータをデータハッシュと比較することによって検証する。復号されたデータの完全性を検証することができなかった場合には、データが傍受され、かつ／又は、不正に操作された可能性があり、そのためこのデータは信頼し得ない。従って、制御はステップＳ９１７に移り、印刷ジョブ全体を廃棄する。制御は次いでステップＳ９１９に渡され終了となる。しかし復号されたデータの完全性がステップＳ９１６で検証された場合には、制御はステップＳ９１８に移り、目的プリンタが復号されたデータに基づいて画像を印刷する（ステップＳ９１２）。制御は次いでステップＳ９１９に至り終了となる。

【００８４】このようにして、目的受信者がいるときにだけ目的画像出力機器で画像を生成することができる安全印刷が提供される。具体的には、目的画像出力機器によって供給される秘密鍵と目的受信者によって供給される秘密鍵との組合せを使用しない限りデータを復号することができない方法で印刷データが暗号化される。

【００８５】本発明を、例示的な特定の実施形態を用い＊て説明した。本発明が上記の実施形態に限定されないこと、及び当業者なら、本発明の趣旨及び範囲から逸脱することなしにさまざまな変更及び修正を実施できることを理解されたい。

【図面の簡単な説明】

【図１】本発明を実施することができるネットワーク化コンピューティング環境を表す図である。

【図２】図１に示した本発明に基づくコンピュータの内部アーキテクチャを示す詳細ブロック図である。

【図３】図１に示した本発明に基づくプリンタの内部アーキテクチャを示す詳細ブロック図である。

【図４】図１に示した本発明に基づくサーバを示す詳細ブロック図である。

【図５Ａ】本発明の第１の実施の形態に基づく安全印刷ジョブのデータ及び対称鍵の暗号化を説明するための図である。

【図５Ｂ】本発明の第２の実施の形態に基づく安全印刷ジョブのデータ暗号化を説明するための図である。

【図５Ｃ】本発明の一実施形態に基づく安全印刷ジョブの復号及び印刷を説明するための図である。

【図５Ｄ】本発明の他の実施形態に基づく安全印刷ジョブの復号及び印刷を説明するための図である。

【図６】本発明の一実施形態に基づく暗号化データ・フォーマットの構造を説明するための図である。

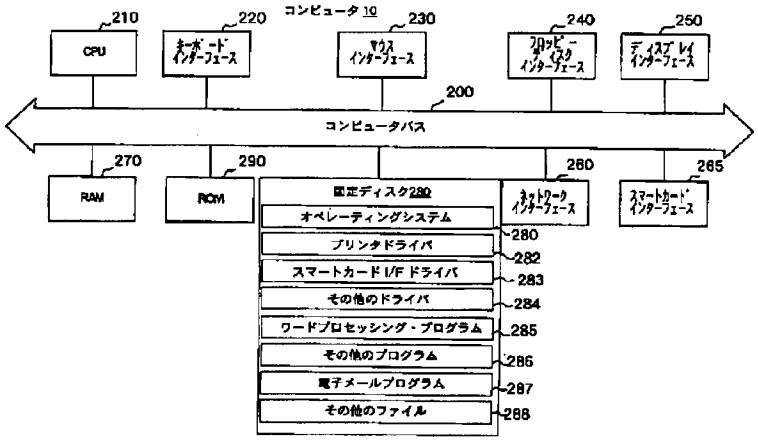
【図７Ａ】本発明の一実施形態に基づく暗号化ヘッダフォーマットの構造を説明するための図である。

【図７Ｂ】本発明の他の実施形態に基づく暗号化ヘッダフォーマットの構造を説明するための図である。

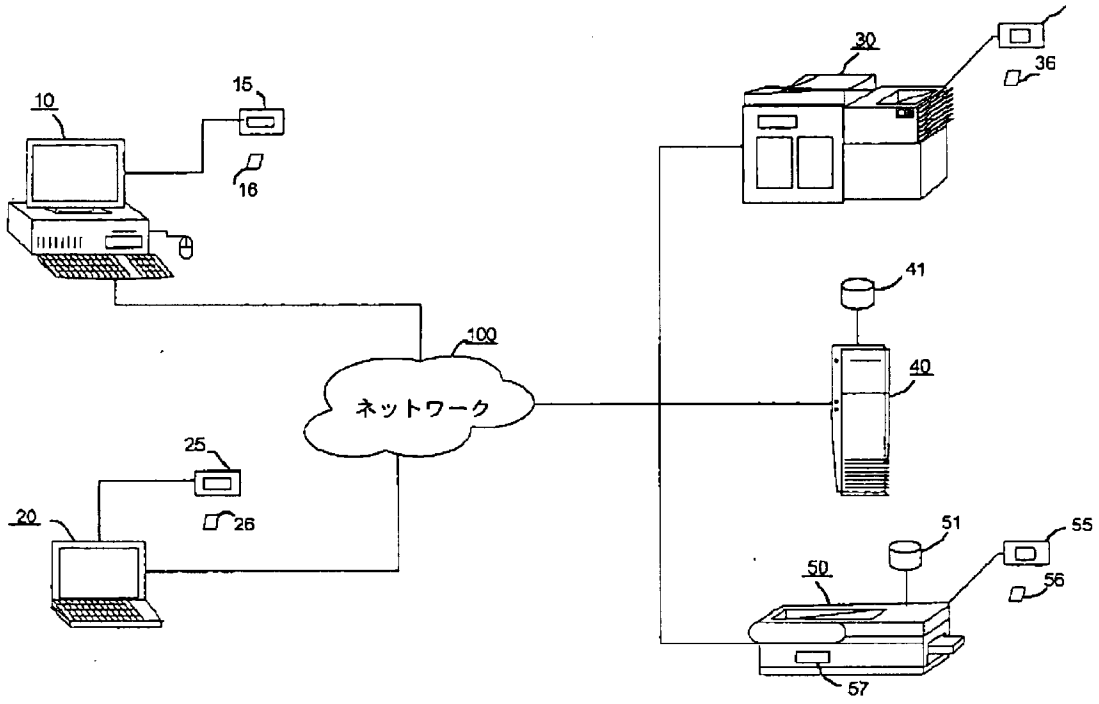
【図８】本発明に基づく安全印刷ジョブの暗号化及び送信を説明するための流れ図である。

【図９】本発明に基づく安全印刷ジョブの復号及び印刷を説明するための流れ図である。

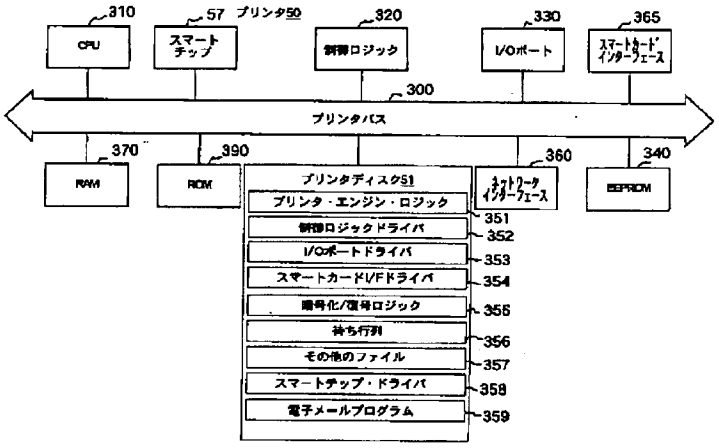
【図２】



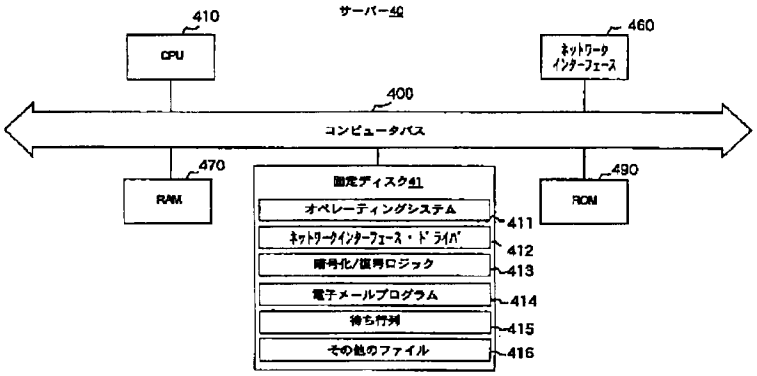
【図１】


10
15
16
30
36
41
40
100
ネットワーク
25
26
20
51
55
50
56
57

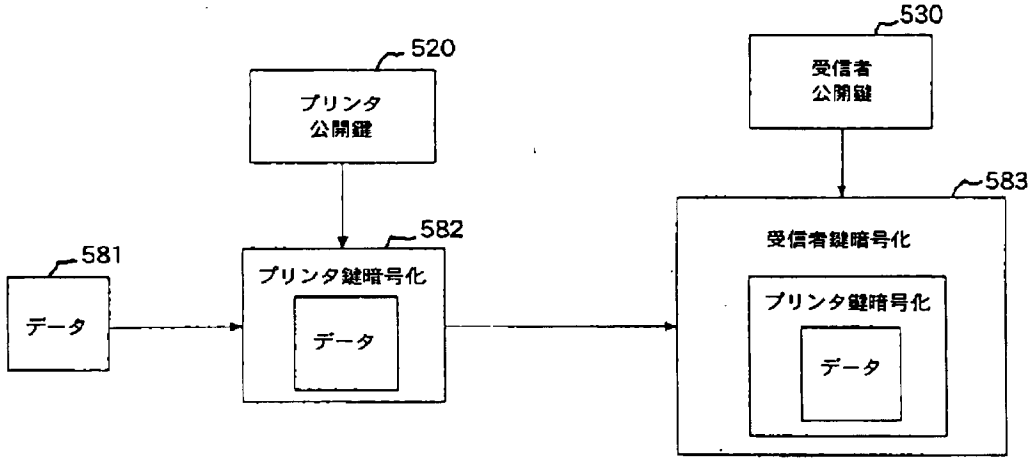
【図３】


310
CPU
57 プリンタ50
スマートチップ
320
制御ロジック
330
I/Oポート
365
スマートカードインターフェース
300
プリンタバス
370
RAM
390
ROM
プリンタディスク51
プリンタ・エンジン・ロジック
351
制御ロジックドライバ
352
I/Oポートドライバ
353
スマートカードI/Fドライバ
354
暗号化/復号ロジック
355
待ち行列
356
その他のファイル
357
スマートチップ・ドライバ
358
電子メールプログラム
359
360
ネットワークインターフェース
340
EEPROM

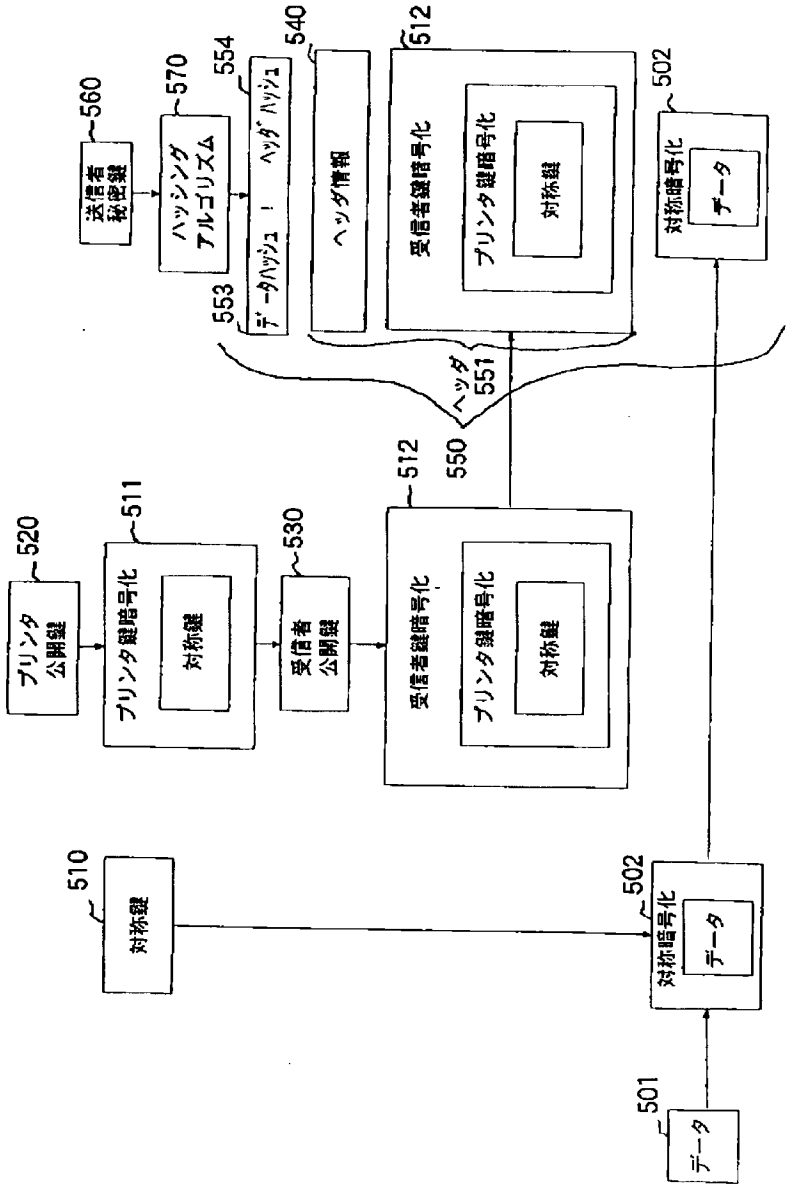
【図４】


410
CPU
サーバー40
460
ネットワーク
インターフェース
400
コンピュータバス
470
RAM
固定ディスク41
オペレーティングシステム
411
ネットワークインターフェース・ドライバ
412
暗号化/復号ロジック
413
電子メールプログラム
414
待ち行列
415
その他のファイル
416
490
ROM

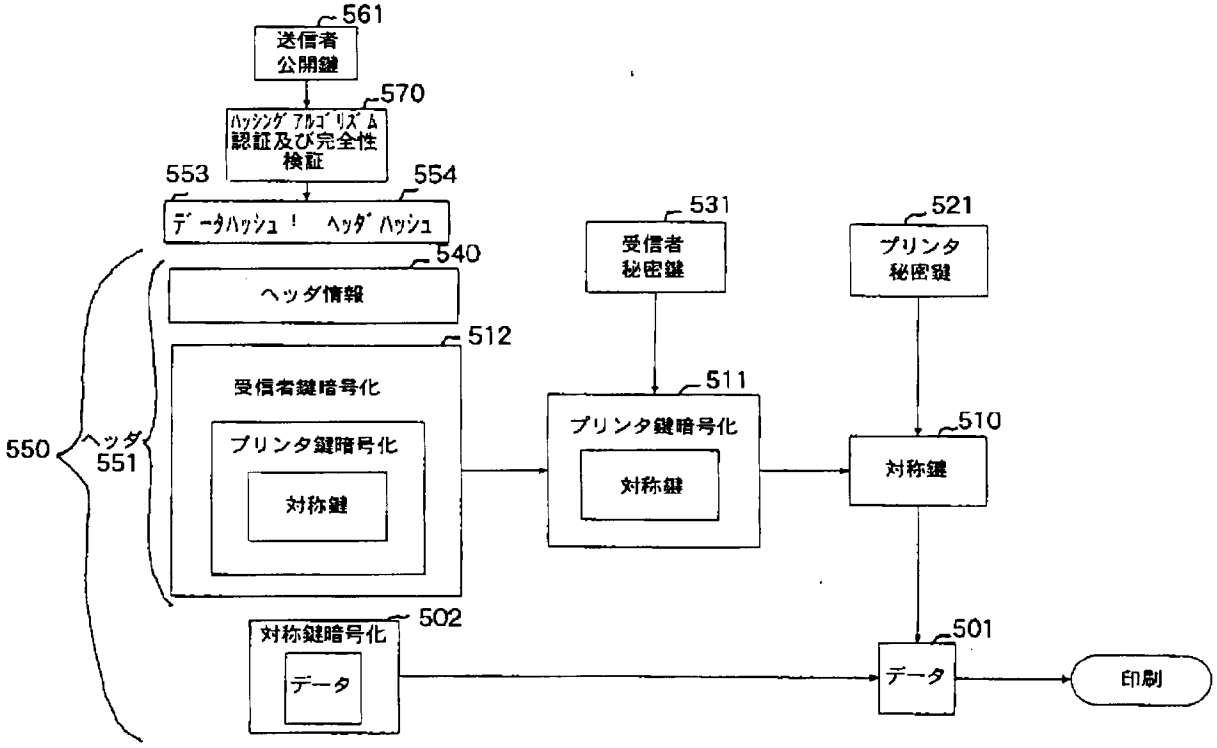
【図５Ｂ】


520
プリンタ
公開鍵
530
受信者
公開鍵
583
受信者鍵暗号化
582
プリンタ鍵暗号化
データ
581
データ
プリンタ鍵暗号化
データ

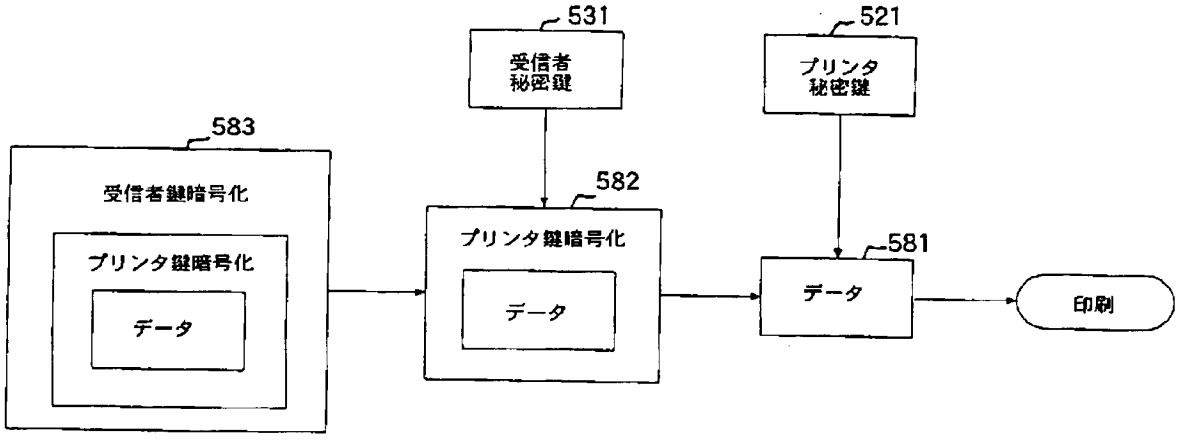
【図５Ａ】


501
データ
502
対称暗号化
データ
510
対称鍵
520
プリンタ公開鍵
511
プリンタ鍵暗号化
対称鍵
530
受信者公開鍵
512
受信者鍵暗号化
プリンタ鍵暗号化
対称鍵
550
ヘッダ
551
553
データハッシュ
554
ヘッダハッシュ
540
ヘッダ情報
512
受信者鍵暗号化
プリンタ鍵暗号化
対称鍵
502
対称暗号化
データ
560
送信者秘密鍵
570
ハッシングアルゴリズム

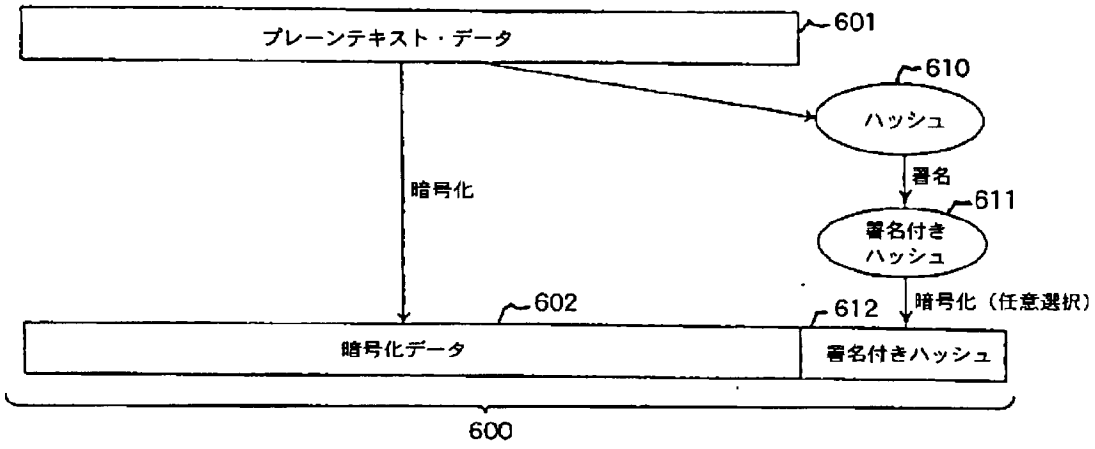
【図５Ｃ】


561
送信者
公開鍵
570
ﾊｯｼﾝｸﾞｱﾙｺﾞﾘｽﾞﾑ
認証及び完全性
検証
553
554
ﾃﾞｰﾀﾊｯｼｭ
ﾍｯﾀﾞﾊｯｼｭ
540
ヘッダ情報
512
受信者鍵暗号化
プリンタ鍵暗号化
対称鍵
550
ヘッダ
551
531
受信者
秘密鍵
511
プリンタ鍵暗号化
対称鍵
521
プリンタ
秘密鍵
510
対称鍵
502
対称鍵暗号化
データ
501
データ
印刷

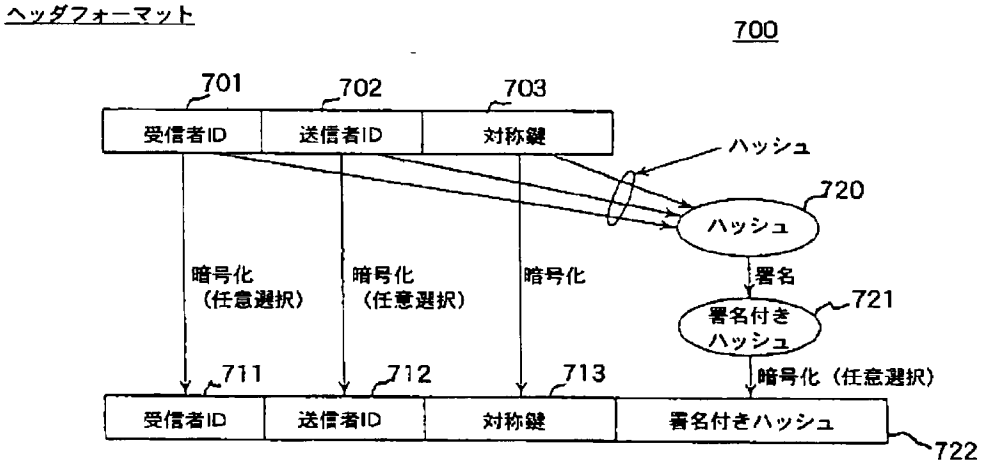
【図５Ｄ】


531
受信者
秘密鍵
521
プリンタ
秘密鍵
583
受信者鍵暗号化
プリンタ鍵暗号化
データ
582
プリンタ鍵暗号化
データ
581
データ
印刷

【図６】

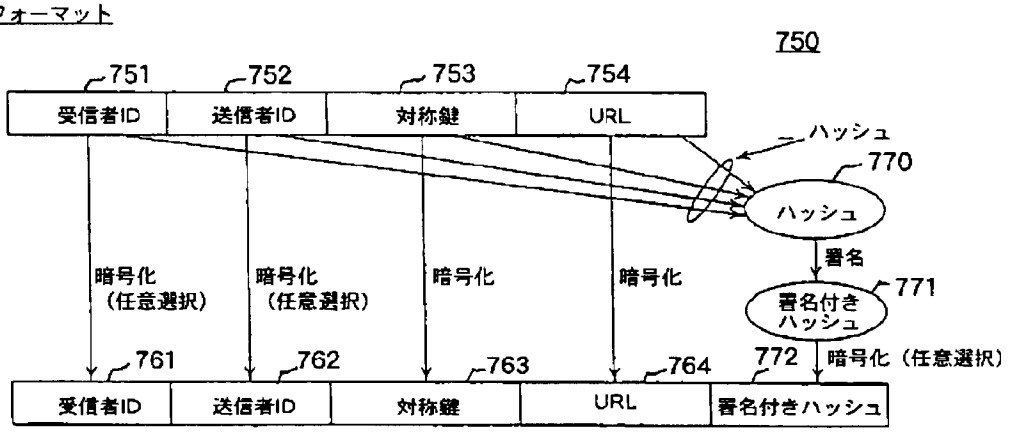

プレーンテキスト・データ
601
610
ハッシュ
署名
611
署名付き
ハッシュ
暗号化
暗号化（任意選択）
602
612
暗号化データ
署名付きハッシュ
600

【図７Ａ】

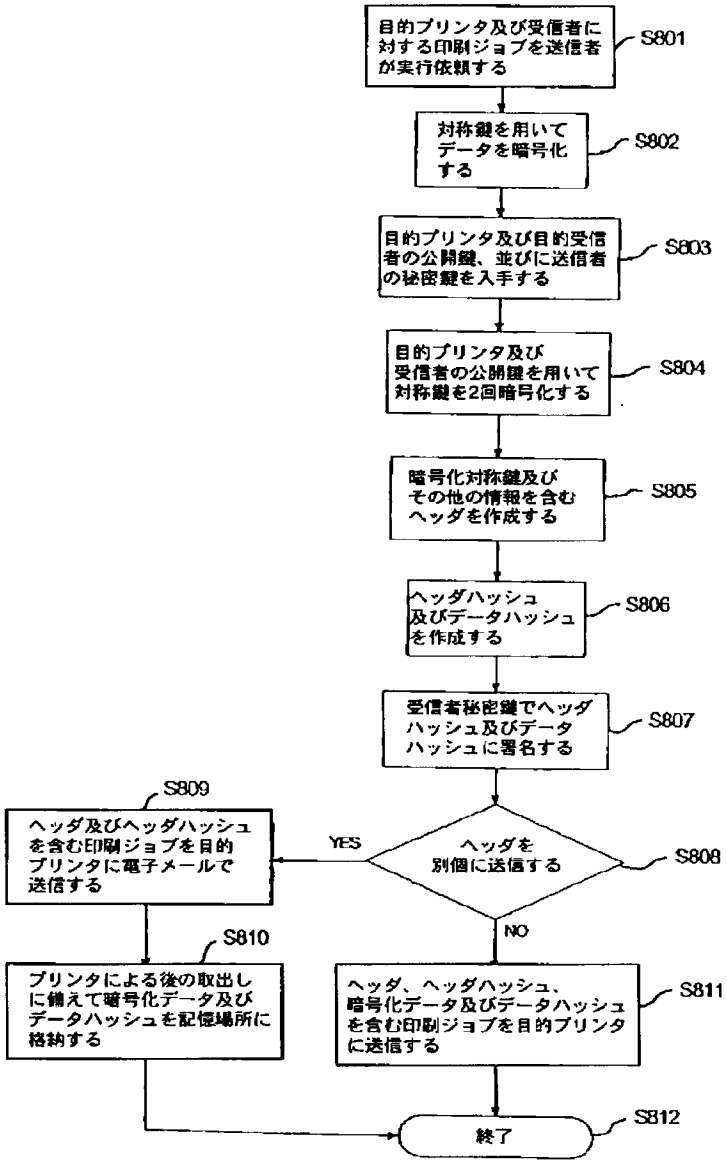

ヘッダフォーマット
700
701
702
703
受信者ID
送信者ID
対称鍵
ハッシュ
720
ハッシュ
暗号化
（任意選択）
暗号化
（任意選択）
暗号化
署名
721
署名付き
ハッシュ
暗号化（任意選択）
711
712
713
受信者ID
送信者ID
対称鍵
署名付きハッシュ
722

【図７Ｂ】

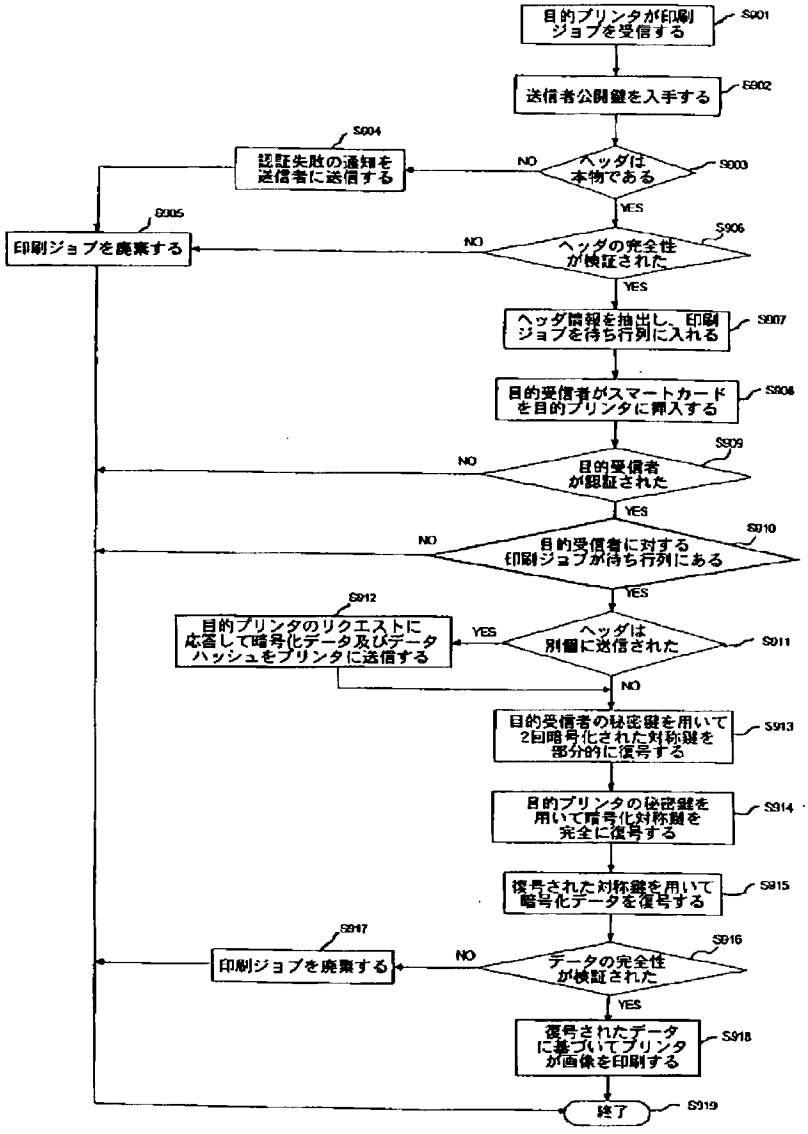
ヘッダフォーマット



【図８】


目的プリンタ及び受信者に対する印刷ジョブを送信者が実行依頼する
S801
対称鍵を用いてデータを暗号化する
S802
目的プリンタ及び目的受信者の公開鍵、並びに送信者の秘密鍵を入手する
S803
目的プリンタ及び受信者の公開鍵を用いて対称鍵を2回暗号化する
S804
暗号化対称鍵及びその他の情報を含むヘッダを作成する
S805
ヘッダハッシュ及びデータハッシュを作成する
S806
受信者秘密鍵でヘッダハッシュ及びデータハッシュに署名する
S807
ヘッダを別個に送信する
S808
YES
NO
S809
ヘッダ及びヘッダハッシュを含む印刷ジョブを目的プリンタに電子メールで送信する
S810
プリンタによる後の取出しに備えて暗号化データ及びデータハッシュを記憶場所に格納する
ヘッダ、ヘッダハッシュ、暗号化データ及びデータハッシュを含む印刷ジョブを目的プリンタに送信する
S811
終了
S812

【図９】



フロントページの続き

(72)発明者　クレイグ　マザガット
アメリカ合衆国　カリフォルニア州　92612,　アーバイン,　イノベーション　ドライブ　110　キヤノン　インフォメーション　システムズ,　インク．内

(72)発明者　ニール　ワイ．イワモト
アメリカ合衆国　カリフォルニア州　92612,　アーバイン,　イノベーション　ドライブ　110　キヤノン　インフォメーション　システムズ,　インク．内

【外国語明細書】

1. Title of Invention

IMAGE OUTPUT METHOD AND APPARATUS THEREOF AND MEDIUM

2. Claims

(1) A method for secure transmission of data to an intended image output device, wherein the data can be used to generate an image at the intended image output device in the presence of an intended recipient, the method comprising:

an encrypting step of twice encrypting the data using a first key and a second key, the first key being a public key of a first private key/public key pair, a private key of the first private key/public key pair being primarily in the sole possession of the intended image output device, and the second key being a public key of a second private key/public key pair, a private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image; and

a transmitting step of transmitting the twice-encrypted data to the intended image output device.

(2) A method for secure transmission of data to an intended image output device, wherein the data can be used to generate an image at the intended image output device in the presence of an intended recipient, the method comprising:

a first encrypting step of encrypting the data using a first key;

a second encrypting step of twice encrypting the first key using a second key and a third key, the second key being a public key of a first private key/public key pair, a private key of the first private key/public key pair being primarily in the sole possession of the intended image output device, and the third key being a public key of a second private

key/public key pair, a private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image; and

a transmitting step of transmitting the encrypted data and the twice-encrypted first key to the intended image output device.

(3) A method according to Claim 2, wherein the first key is randomly generated.

(4) A method according to Claim 2, wherein the first encrypting step utilizes a symmetric encryption algorithm.

(5) A method according to Claim 2, wherein the second encrypting step utilizes an asymmetric encryption algorithm.

(6) A method according to Claim 2, wherein the second encrypting step encrypts the first key using the second key before encrypting the first key using the third key.

(7) A method according to Claim 2, wherein the second encrypting step encrypts the first key using the third key before encrypting the first key using the second key.

(8) A method according to Claim 2, wherein, in the transmitting step, the twice-encrypted first key is contained in a header which also contains information related to the identity of a device initiating the secure transmission.

(9) A method according to Claim 2, wherein, in the transmitting step, th

e twice-encrypted first key is contained in a header which also contains information related to the identity of a person initiating the secure transmission.

(10) A method according to Claim 9, further comprising:

a hashing step of processing the header and the encrypted data with a hashing algorithm, resulting in a header hash and a data hash; and

a signing step of digitally signing the header hash and the data hash with a private key of a third private key/public key pair, the private key of the third private key/public key pair being primarily maintained in the sole possession of the person initiating the secure transmission,

wherein the transmitting step further transmits the signed header hash and the signed data hash.

(11) A method according to Claim 2, wherein the intended image output device is a printer.

(12) A method according to Claim 2, wherein the intended image output device is a facsimile machine.

(13) A method for secure transmission of data to an intended image output device, wherein the data can be used to generate an image at the intended image output device in the presence of an intended recipient, the method comprising:

a first encrypting step of encrypting the data using a first key;

a second encrypting step of twice encrypting the first key using a second key and a third key, the second key being a public key of a first private key/public key pair, a private key of the first private key/publ

ic key pair being primarily in the sole possession of the intended image output device, and the third key being a public key of a second private key/public key pair, a private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image;

a generating step of generating a header containing the twice-encrypted first key;

a first transmitting step of transmitting the header to the intended image output device;

a receiving step of receiving a request from the intended image output device for the encrypted data; and

a second transmitting step of transmitting the encrypted data to the intended image output device.

(14) A method according to Claim 13, wherein the first transmitting step transmits the header to the intended image output device by e-mail.

(15) A method according to Claim 13, wherein the header which is generated in the generating step also contains a reference to a location of the encrypted data, and wherein the request for encrypted data contains the reference to the location of the encrypted data.

(16) A method for generating an image from twice-encrypted data transmitted to an intended image output device, wherein the twice-encrypted data can be used to generate the image at the intended image output device in the presence of an intended recipient, the method comprising:

a receiving step of receiving twice-encrypted data;

a decrypting step of twice decrypting the twice-encrypted data using a first key and a second key, the first key being a private key of a fi

rst private key/public key pair, the private key of the first private ke y/public key pair being primarily in the sole possession of the intended recipient of the image, and the second key being a private key of a sec ond private key/public key pair, the private key of the second private k ey/public key pair being primarily in the sole possession of the intende d image output device; and

an image generating step of generating an image from the decrypted d ata.

(17) A method for generating an image from data transmitted to an intend ed image output device, wherein the data can be used to generate the ima ge at the intended image output device in the presence of an intended re cipient, the method comprising:

a receiving step of receiving encrypted data and a twice-encrypted f irst key;

a first decrypting step of twice decrypting the twice-encrypted firs t key using a second key and a third key, the second key being a private key of a first private key/public key pair, the private key of the firs t private key/public key pair being primarily in the sole possession of the intended recipient of the image, and the third key being a private k ey of a second private key/public key pair, the private key of the secon d private key/public key pair being primarily in the sole possession of the intended image output device;

a second decrypting step of decrypting the encrypted data using the decrypted first key; and

an image generating step of generating an image from the decrypted d ata.

(18) A method according to Claim 17, wherein the first decrypting step u

tilizes an asymmetric decryption algorithm.

(19) A method according to Claim 17, wherein the second decrypting step utilizes a symmetric decryption algorithm.

(20) A method according to Claim 17, wherein the first decrypting step decrypts the twice-encrypted first key using the second key before decrypting the twice-encrypted first key using the third key.

(21) A method according to Claim 17, wherein the first decrypting step decrypts the twice-encrypted first key using the third key before decrypting the twice-encrypted first key using the second key.

(22) A method according to Claim 17, wherein the third key is contained within the intended image output device, whereby the third key is primarily shielded from access by devices other than the intended image output device.

(23) A method according to Claim 17, wherein the second key is contained in a smart-card possessed by the intended recipient, whereby the second key is hidden from recipients other than the intended recipient.

(24) A method according to Claim 17, wherein the receiving step further receives a signed header hash and a signed data hash, the method further comprising a verifying step of verifying the authenticity and the integrity of the signed header hash and of the signed data hash.

(25) A method according to Claim 24, further comprising the step of discarding the encrypted data rather than outputting an image based upon the

encrypted data, if the signed header hash or the signed data hash fail the verification of authenticity and integrity.

(26) A method according to Claim 25, further comprising the step of sending a notice to a sender of the signed header, if the signed header hash or the signed data hash fail the verification of authenticity and integrity.

(27) A method according to Claim 17, wherein the intended image output device is a printer.

(28) A method according to Claim 17, wherein the intended image output device is a facsimile machine.

(29) A method for generating an image from data transmitted to an intended image output device, wherein the data can be used to generate the image at the intended image output device in the presence of an intended recipient, the method comprising:

a receiving step of receiving a header containing a twice-encrypted first key;

a sending step of sending a request for encrypted data corresponding to the header;

a receiving step of receiving encrypted data corresponding to the header;

a first decrypting step of twice decrypting the twice-encrypted first key using a second key and a third key, the second key being a private key of a first private key/public key pair, the private key of the first private key/public key pair being primarily in the sole possession of the intended recipient of the image, and the third key being a private k

ey of a second private key/public key pair, the private key of the secon d private key/public key pair being primarily in the sole possession of the intended image output device;

a second decrypting step of decrypting the encrypted data using the decrypted first key; and

an image generating step of generating an image from the decrypted d ata.

(30) A method according to Claim 29, wherein the header is received in t he receiving step by e-mail.

(31) A method according to Claim 29, wherein the header also contains a reference to a location of the encrypted data, and wherein the request f or encrypted data contains the reference to the location of the encrypte d data.

(32) An apparatus for secure transmission of data to an intended image o utput device, wherein the data can be used to generate an image at the i ntended image output device for receipt by an intended recipient, the ap paratus comprising:

a memory including a region for storing executable process steps and data for the image; and

a processor for executing the executable process steps;

wherein the executable process steps include (a) an encrypting step of twice encrypting the data using a first key and a second key, the fir st key being a public key of a first private key/public key pair, a priv ate key of the first private key/public key pair being primarily in the sole possession of the intended image output device, and the second key being a public key of a second private key/public key pair, a private ke

y of the second private-key/public key pair being primarily in the sole possession of the intended recipient of the image; and (b) a transmitting step of transmitting the twice-encrypted data to the intended image output device.

(33) An apparatus for secure transmission of data to an intended image output device, wherein the data can be used to generate an image at the intended image output device in the presence of an intended recipient, the apparatus comprising:

a memory including a region for storing executable process steps and data for the image; and

a processor for executing the executable process steps;

wherein the executable process steps include (a) a first encrypting step of encrypting the data using a first key; (b) a second encrypting step of twice encrypting the first key using a second key and a third key, the second key being a public key of a first private key/public key pair, a private key of the first private key/public key pair being primarily in the sole possession of the intended image output device, and the third key being a public key of a second private key/public key pair, a private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image; and (c) a transmitting step of transmitting the encrypted data and the twice-encrypted first key to the intended image output device.

(34) An apparatus according to Claim 33, wherein the first key is randomly generated.

(35) An apparatus according to Claim 33, wherein the first encrypting step utilizes a symmetric encryption algorithm.

(36) An apparatus according to Claim 33, wherein the second encrypting step utilizes an asymmetric encryption algorithm.

(37) An apparatus according to Claim 33, wherein the second encrypting step encrypts the first key using the second key before encrypting the first key using the third key.

(38) An apparatus according to Claim 33, wherein the second encrypting step encrypts the first key using the third key before encrypting the first key using the second key.

(39) An apparatus according to Claim 33, wherein, in the transmitting step, the twice-encrypted first key is contained in a header which also contains information related to the identity of a device initiating the secure transmission.

(40) An apparatus according to Claim 33, wherein, in the transmitting step, the twice-encrypted first key is contained in a header which also contains information related to the identity of a person initiating the secure transmission.

(41) An apparatus according to Claim 40, wherein the executable process steps further comprise: (d) a hashing step of processing the header and the encrypted data with a hashing algorithm, resulting in a header hash and a data hash; and (e) a signing step of digitally signing the header hash and the data hash with a private key of a third private key/public key pair, the private key of the third private key/public key pair being primarily maintained in the sole possession of the person initiating th

e secure transmission, wherein the transmitting step further transmits t he signed header hash and the signed data hash.

(42) An apparatus according to Claim 33, wherein the apparatus is a comp uter and the intended image output device is a printer.

(43) An apparatus according to Claim 33, wherein the apparatus is a comp uter and the intended image output device is a facsimile machine.

(44) An apparatus according to Claim 33, wherein the apparatus is a firs t facsimile machine and the intended image output device is a second fac simile machine.

(45) An apparatus for secure transmission of data to an intended image o utput device, wherein the data can be used to generate an image at the i ntended image output device in the presence of an intended recipient, th e apparatus comprising:

a memory including a region for storing executable process steps and data for the image; and

a processor for executing the executable process steps;

wherein the executable process steps include (a) a first encrypting step of encrypting the data using a first key; (b) a second encrypting s tep of twice encrypting the first key using a second key and a third key , the second key being a public key of a first private key/public key pa ir, a private key of the first private key/public key pair being primari ly in the sole possession of the intended image output device, and the t hird key being a public key of a second private key/public key pair, a p rivate key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image; (c) a genera

ting step of generating a header containing the twice-encrypted first key; (d) a first transmitting step of transmitting the header to the intended image output device; (e) a receiving step of receiving a request from the intended image output device for the encrypted data; and (f) a second transmitting step of transmitting the encrypted data to the intended image output device.

(46) A method according to Claim 45, wherein the first transmitting step transmits the header to the intended image output device by e-mail.

(47) A method according to Claim 45, wherein the header which is generated in the generating step also contains a reference to a location of the encrypted data, and wherein the request for encrypted data contains the reference to the location of the encrypted data.

(48) An image output device for generating an image from data transmitted to the image output device, wherein the data can be used to generate the image at the image output device in the presence of an intended recipient, the image output device comprising:

a receiver for receiving twice-encrypted data;

an image generator for generating an image from image data;

a memory including a region for storing executable process steps and data; and

a processor for executing the executable process steps, wherein the executable process steps include: (a) a decrypting step of twice decrypting the twice-encrypted data using a first key and a second key, the first key being a private key of a first private key/public key pair, the private key of the first private key/public key pair being primarily in the sole possession of the intended recipient of the image, and the seco

od key being a private key of a second private key/public key pair, the private key of the second private key/public key pair being primarily in the sole possession of the intended image output device; and (b) an image generating step of generating an image from the decrypted data.

(49) An image output device for generating an image from data transmitted to the image output device, wherein the data can be used to generate the image at the image output device in the presence of an intended recipient, the image output device comprising:

a receiver for receiving encrypted data and an twice-encrypted first key;

an image generator for generating an image from image data;

a memory including a region for storing executable process steps and data; and

a processor for executing the executable process steps, wherein the executable process steps include: (a) a first decrypting step of decrypting the twice-encrypted first key using a second key and a third key, the second key being a private key of a first private key/public key pair, the private key of the first private key/public key pair being primarily in the sole possession of the intended recipient of the image, and the third key being a private key of a second private key/public key pair, the private key of the second private key/public key pair being primarily in the sole possession of the intended image output device; (b) a second decrypting step of decrypting the encrypted data using the decrypted first key; and (c) an image generating step of generating an image from the decrypted data using the image generator.

(50) An image output device according to Claim 49, wherein the first decrypting step utilizes an asymmetric decryption algorithm.

(51) An image output device according to Claim 49, wherein the second decrypting step utilizes a symmetric decryption algorithm.

(52) An image output device according to Claim 49, wherein the first decrypting step decrypts the first key using the second key before decrypting the first key using the third key.

(53) An image output device according to Claim 49, wherein the first decrypting step decrypts the first key using the third key before decrypting the first key using the second key.

(54) An image output device according to Claim 49, wherein the third key is contained within the image output device, whereby the third key is primarily shielded from access by devices other than the image output device.

(55) An image output device according to Claim 49, wherein the second key is contained in a smart-card possessed by the intended recipient, whereby the second key is hidden from recipients other than the intended recipient.

(56) An image output device according to Claim 49, wherein the receiving step further receives a signed header hash and a signed data hash, the executable process steps further comprising a verifying step of verifying the authenticity and integrity of the signed header hash and of the signed data hash.

(57) An image output device according to Claim 56, wherein the executabl

e process steps further comprise the step of discarding the encrypted da ta rather than outputting an image, if the signed header hash or the sig ned data hash fail the verification of authenticity and integrity.

(58) An image output device to Claim 57, wherein the executable process steps further comprise the step of sending a notice to a sender of the s igned header, if the signed header hash or the signed data hash fail the verification of authenticity and integrity.

(59) An image output device according to Claim 49, wherein the image out put device is a printer.

(60) An image output device according to Claim 49, wherein the image out put device is a facsimile machine.

(61) An image output device for generating an image from data transmitte d to the image output device, wherein the data can be used to generate t he image at the image output device in the presence of an intended recip ient, the image output device comprising:

a receiver for receiving a header containing a twice-encrypted first key;

an image generator for generating an image from image data;

a memory including a region for storing executable process steps and data; and

a processor for executing the executable process steps, wherein the executable process steps include: (a) a sending step of sending a reque st for encrypted data corresponding to the header; (b) a receiving step of receiving encrypted data corresponding to the header; (c) a first dec rypting step of twice decrypting the twice-encrypted first key using a s

econd key and a third key, the second key being a private key of a first private key/public key pair, the private key of the first private key/public key pair being primarily in the sole possession of the intended recipient of the image, and the third key being a private key of a second private key/public key pair, the private key of the second private key/public key pair being primarily in the sole possession of the intended image output device; (d) a second decrypting step of decrypting the encrypted data using the decrypted first key; and (e) an image generating step of generating an image from the decrypted data.

(62) A method according to Claim 61, wherein the header is received by e-mail.

(63) A method according to Claim 61, wherein the header also contains a reference to a location of the encrypted data, and wherein the request for encrypted data contains the reference to the location of the encrypted data.

(64) A computer-readable medium which stores computer-executable process steps which securely transmit data to an intended image output device, wherein the data can be used to generate an image at the intended image output device in the presence of an intended recipient, the computer-executable process steps comprising:

a data generating step to generate data for an image;

an encrypting step to twice encrypt the data using a first key and a second key, the first key being a public key of a first private key/public key pair, a private key of the first private key/public key pair being primarily in the sole possession of the intended image output device, and the second key being a public key of a second private key/public ke

y pair, a private key of the second private key/public key pair being pr imarily in the sole possession of the intended recipient of the image; a nd

a transmitting step to transmit the twice-encrypted data to the inte nded image output device.

(65) A computer-readable medium which stores computer-executable process steps which securely transmit data to an intended image output device, wherein the data can be used to generate an image at the intended image output device in the presence of an intended recipient, the computer-exe cutable process steps comprising:

a data generating step to generate data for an image;

a first encrypting step to encrypt the data using a first key;

a second encrypting step to encrypt the first key twice using a seco nd key and a third key, the second key being a public key of a first pri vate key/public key pair, a private key of the first private key/public key pair being primarily in the sole possession of the intended image ou tput device, and the third key being a public key of a second private ke y/public key pair, a private key of the second private key/public key pa ir being primarily in the sole possession of the intended recipient of t he image; and

a transmitting step to transmit the encrypted data and the twice-enc rypted first key to the intended image output device.

(66) A computer-readable medium according to Claim 65, wherein the first key is randomly generated.

(67) A computer-readable medium according to Claim 65, wherein the first encrypting step utilizes a symmetric encryption algorithm.

(68) A computer-readable medium according to Claim 65, wherein the second encrypting step utilizes an asymmetric encryption algorithm.

(69) A computer-readable medium according to Claim 65, wherein the second encrypting step encrypts the first key using the second key before encrypting the first key using the third key.

(70) A computer-readable medium according to Claim 65, wherein the second encrypting step encrypts the first key using the third key before encrypting the first key using the second key.

(71) A computer-readable medium according to Claim 65, wherein, in the transmitting step, the twice-encrypted first key is contained in a header which also contains information related to the identity of a device initiating the secure transmission.

(72) A computer-readable medium according to Claim 65, wherein, in the transmitting step, the twice encrypted first key is contained in a header which also contains information related to the identity of a person initiating the secure transmission.

(73) A computer-readable medium according to Claim 72, wherein the computer-executable process steps further comprise:

a hashing step to process the header and the encrypted data with a hashing algorithm, resulting in a header hash and a data hash; and

a signing step to digitally sign the header hash and the data hash with a private key of a third private key/public key pair, the private key of the third private key/public key pair being primarily maintained in

the sole possession of the person initiating the secure transmission,

wherein the transmitting step further transmits the signed header hash and the signed data hash.

(74) A computer-readable medium according to Claim 65, wherein the intended image output device is a printer.

(75) A computer-readable medium according to Claim 65, wherein the intended image output device is a facsimile machine.

(76) A computer-readable medium which stores computer-executable process steps which securely transmit data to an intended image output device, wherein the data can be used to generate an image at the intended image output device in the presence of an intended recipient, the computer-executable process steps comprising:

a data generating step to generate data for an image;

a first encrypting step to encrypt the data using a first key;

a second encrypting step to twice encrypt the first key using a second key and a third key, the second key being a public key of a first private key/public key pair, a private key of the first private key/public key pair being primarily in the sole possession of the intended image output device, and the third key being a public key of a second private key/public key pair, a private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image;

a generating step to generate a header containing the twice-encrypted first key;

a first transmitting step to transmit the header to the intended image output device;

a receiving step to receive a request from the intended image output device for the encrypted data; and

a second transmitting step to transmit the encrypted data to the intended image output device.

(77) A computer-readable medium according to Claim 76, wherein the first transmitting step transmits the header to the intended image output device by e-mail.

(78) A computer-readable medium according to Claim 76, wherein the header which is generated in the generating step also contains a reference to a location of the encrypted data, and wherein the request for encrypted data contains the reference to the location of the encrypted data.

(79) A computer-readable medium which stores computer-executable process steps for generating an image from twice-encrypted data transmitted to an intended image output device, wherein the twice-encrypted data can be used to generate the image at the intended image output device in the presence of an intended recipient, the computer-executable process steps comprising:

a receiving step to receive twice-encrypted data;

a decrypting step to twice decrypt the twice-encrypted data using a first key and a second key, the first key being a private key of a first private key/public key pair, the private key of the first private key/public key pair being primarily in the sole possession of the intended recipient of the image, and the second key being a private key of a second private key/public key pair, the private key of the second private key/public key pair being primarily in the sole possession of the intended image output device; and

an image generating step to generate an image from the decrypted dat
a.

(80) A computer-readable medium which stores computer-executable process steps for generating an image from data transmitted to an intended imag e output device, wherein the data can be used to generate the image at t he intended image output device in the presence of an intended recipient , the computer-executable process steps comprising:

a receiving step to receive encrypted data and a twice-encrypted fir st key;

a first decrypting step to twice decrypt the twice-encrypted first k ey using a second key and a third key, the second key being a private ke y of a first private key/public key pair, the private key of the first p rivate key/public key pair being primarily in the sole possession of the intended recipient of the image, and the third key being a private key of a second private key/public key pair, the private key of the second p rivate key/public key pair being primarily in the sole possession of the intended image output device;

a second decrypting step to decrypt the encrypted data using the dec rypted first key; and

an image generating step to generate an image from the decrypted dat
a.

(81) A computer-readable medium according to Claim 80, wherein the first decrypting step utilizes an asymmetric decryption algorithm.

(82) A computer-readable medium according to Claim 80, wherein the secon d decrypting step utilizes a symmetric decryption algorithm.

(83) A computer-readable medium according to Claim 80, wherein the first decrypting step decrypts the twice-encrypted first key using the second key before decrypting the twice-encrypted first key using the third key .

(84) A computer-readable medium according to Claim 80, wherein the first decrypting step decrypts the twice-encrypted first key using the third key before decrypting the twice-encrypted first key using the second key .

(85) A computer-readable medium according to Claim 80, wherein the third key is contained within the intended image output device, whereby the t hird key is primarily shielded from access by devices other than the int ended image output device.

(86) A computer-readable medium according to Claim 80, wherein the secon d key is contained in a smart-card possessed by the intended recipient, whereby the second key is hidden from recipients other than the intended recipient.

(87) A computer-readable medium according to Claim 80, wherein the recei ving step further receives a signed header hash and a signed data hash, the method further comprising a verifying step of verifying the authenti city and the integrity of the signed header hash and of the signed data hash.

(88) A computer-readable medium according to Claim 87, further comprisin g the step of discarding the encrypted data rather than outputting an im age based upon the encrypted data, if the signed header hash or the sign

ed data hash fail the verification of authenticity and integrity.

(89) A computer-readable medium according to Claim 88, further comprising the step of sending a notice to a sender of the signed header, if the signed header hash or the signed data hash fail the verification of authenticity and integrity.

(90) A computer-readable medium according to Claim 80, wherein the intended image output device is a printer.

(91) A computer-readable medium according to Claim 80, wherein the intended image output device is a facsimile machine.

(92) A computer-readable medium which stores computer-executable process steps for generating an image from data transmitted to an intended image output device, wherein the data can be used to generate the image at the intended image output device in the presence of an intended recipient, the computer-executable process steps comprising:

a receiving step to receive a header containing a twice-encrypted first key;

a sending step to send a request for encrypted data corresponding to the header;

a receiving step to receive encrypted data corresponding to the header;

a first decrypting step to twice decrypt the twice-encrypted first key using a second key and a third key, the second key being a private key of a first private key/public key pair, the private key of the first private key/public key pair being primarily in the sole possession of the intended recipient of the image, and the third key being a private key

of a second private key/public key pair, the private key of the second p
rivate key/public key pair being primarily in the sole possession of the
intended image output device;

a second decrypting step to decrypt the encrypted data using the dec
rypted first key; and

an image generating step to generate an image from the decrypted dat
a.

(93) A computer-readable medium according to Claim 92, wherein the heade
r is received in the receiving step by e-mail.

(94) A method according to Claim 92, wherein the header also contains a
reference to a location of the encrypted data, and wherein the request f
or encrypted data contains the reference to the location of the encrypte
d data.

(95) A printer driver which securely transmits data to an intended print
er, wherein the data can be used to generate an image at the intended pr
inter in the presence of an intended recipient, the printer driver compr
ising:

data generating code for generating data for an image;

encrypting code for twice encrypting the data using a first key and
a second key, the first key being a public key of a first private key/pu
blic key pair, a private key of the first private key/public key pair be
ing primarily in the sole possession of the intended image output device
, and the second key being a public key of a second private key/public k
ey pair, a private key of the second private key/public key pair being p
rimarily in the sole possession of the intended recipient of the image;
and

transmitting code for transmitting the twice-encrypted data to the intended image output device.

(96) A printer driver which securely transmits data to an intended printer, wherein the data can be used to generate an image at the intended printer in the presence of an intended recipient, the printer driver comprising:

data generating code for generating data for an image;

first encrypting code for encrypting the data using a first key;

second encrypting code for twice encrypting the first key using a second key and a third key, the second key being a public key of a first private key/public key pair, a private key of the first private key/public key pair being primarily in the sole possession of the intended image output device, and the third key being a public key of a second private key/public key pair, a private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image; and

transmitting code for transmitting the encrypted data and the twice-encrypted first key to the intended printer.

(97) A printer driver according to Claim 96, wherein the first key is randomly generated.

(98) A printer driver according to Claim 96, wherein the first encrypting code utilizes a symmetric encryption algorithm.

(99) A printer driver according to Claim 96, wherein the second encrypting code utilizes an asymmetric encryption algorithm.

(100) A printer driver according to Claim 96, wherein the second encrypting code encrypts the first key using the second key before encrypting the first key using the third key.

(101) A printer driver according to Claim 96, wherein the second encrypting code encrypts the first key using the third key before encrypting the first key using the second key.

(102) A printer driver according to Claim 96, wherein the twice-encrypted first key is contained in a header which also contains information related to the identity of a person initiating the secure transmission.

(103) A printer driver according to Claim 102, wherein the header also contains a signed header hash and a signed data hash, and further comprising verification code for verification of the authenticity and integrity of the signed header hash and of the signed data hash.

(104) A printer driver according to Claim 103, further comprising sending code for sending a notice to a sender of the header, if one of the signed header hash and signed data hash fails the verification of authenticity and integrity.

(105) A printer driver which securely transmits data to an intended printer, wherein the data can be used to generate an image at the intended printer in the presence of an intended recipient, the printer driver comprising:

data generating code for generating data for an image;

first encrypting code for encrypting the data using a first key;

second encrypting code for twice encrypting the first key using a se

cond key and a third key, the second key being a public key of a first p rivate key/public key pair, a private key of the first private key/publi c key pair being primarily in the sole possession of the intended image output device, and the third key being a public key of a second private key/public key pair, a private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image;

generating code for generating a header containing the twice-encrypt ed first key;

first transmitting code for transmitting the header to the intended image output device;

receiving code for receiving a request from the intended image outpu t device for the encrypted data; and

second transmitting code for transmitting the encrypted data to the intended image output device.

(106) A printer driver according to Claim 105, wherein the first transmi tting code transmits the header to the intended image output device by e -mail.

(107) A printer driver according to Claim 105, wherein the header which is generated in the generating code also contains a reference to a locat ion of the encrypted data, and wherein the request for encrypted data co ntains the reference to the location of the encrypted data.

(108) Computer-executable process steps stored on a computer-readable me dium, the computer-executable process steps for generating an image from twice-encrypted data transmitted to an intended image output device, wh erein the twice-encrypted data can be used to generate the image at the

intended image output device in the presence of an intended recipient, said computer-executable process steps comprising:

receiving code to receive twice-encrypted data;

decrypting code to twice decrypt the twice-encrypted data using a first key and a second key, the first key being a private key of a first private key/public key pair, the private key of the first private key/public key pair being primarily in the sole possession of the intended recipient of the image, and the second key being a private key of a second private key/public key pair, the private key of the second private key/public key pair being primarily in the sole possession of the intended image output device; and

an image generating code to generate an image from the decrypted data.

(109) Computer-executable process steps stored on a computer-readable medium, the computer-executable process steps for generating an image from twice-encrypted data transmitted to an intended image output device, wherein the twice-encrypted data can be used to generate the image at the intended image output device in the presence of an intended recipient, said computer-executable process steps comprising:

receiving code to receive encrypted data and a twice-encrypted first key;

first decrypting code to twice decrypt the twice-encrypted first key using a second key and a third key, the second key being a private key of a first private key/public key pair, the private key of the first private key/public key pair being primarily in the sole possession of the intended recipient of the image, and the third key being a private key of a second private key/public key pair, the private key of the second private key/public key pair being primarily in the sole possession of the i

ntended image output device;

second decrypting code to decrypt the encrypted data using the decrypted first key; and

image generating code to generate an image from the decrypted data.

(110) Computer-executable process steps according to Claim 109, wherein the first decrypting code utilizes an asymmetric decryption algorithm.

(111) Computer-executable process steps according to Claim 109, wherein the second decrypting code utilizes a symmetric decryption algorithm.

(112) Computer-executable process steps according to Claim 109, wherein the first decrypting code decrypts the twice-encrypted first key using the second key before decrypting the twice-encrypted first key using the third key.

(113) Computer-executable process steps according to Claim 109, wherein the first decrypting code decrypts the twice-encrypted first key using the third key before decrypting the twice-encrypted first key using the second key.

(114) Computer-executable process steps according to Claim 109, wherein the third key is contained within the intended image output device, whereby the third key is primarily shielded from access by devices other than the intended image output device.

(115) Computer-executable process steps according to Claim 109, wherein the second key is contained in a smart-card possessed by the intended recipient, whereby the second key is hidden from recipients other than the

intended recipient.

(116) Computer-executable process steps according to Claim 109, wherein the receiving code further receives a signed header hash and a signed data hash, the method further comprising verifying code to verify the authenticity and the integrity of the signed header hash and of the signed data hash.

(117) Computer-executable process steps according to Claim 116, further comprising code to discard the encrypted data rather than outputting an image based upon the encrypted data, if the signed header hash or the signed data hash fail the verification of authenticity and integrity.

(118) Computer-executable process steps according to Claim 117, further comprising code to send a notice to a sender of the signed header, if the signed header hash or the signed data hash fail the verification of authenticity and integrity.

(119) Computer-executable process steps according to Claim 109, wherein the intended image output device is a printer.

(120) Computer-executable process steps according to Claim 109, wherein the intended image output device is a facsimile machine.

(121) Computer-executable process steps stored on a computer-readable medium, the computer-executable process steps for generating an image from data transmitted to an intended image output device, wherein the data can be used to generate the image at the intended image output device in the presence of an intended recipient, the computer-executable process s

teps comprising:

receiving code to receive a header containing a twice-encrypted firs t key;

sending code to send a request for encrypted data corresponding to t he header;

receiving code to receive encrypted data corresponding to the header ;

first decrypting code to twice decrypt the twice encrypted first key using a second key and a third key, the second key being a private key of a first private key/public key pair, the private key of the first pri vate key/public key pair being primarily in the sole possession of the i ntended recipient of the image, and the third key being a private key of a second private key/public key pair, the private key of the second pri vate key/public key pair being primarily in the sole possession of the i ntended image output device;

second decrypting code to decrypt the encrypted data using the decry pted first key; and

image generating code to generate an image from the decrypted data.

(122) Computer-executable process steps according to Claim 121, wherein the header is received by e-mail.

(123) Computer-executable process steps according to Claim 121, wherein the header also contains a reference to a location of the encrypted data , and wherein the request for encrypted data contains the reference to t he location of the encrypted data.

3. Detailed explanation of the invention

Field Of The Invention

The present invention is related to an image output method and apparatus thereof and computer-readable medium which perform secure printing wherein an image can be generated only by an intended image output device in the presence of an intended recipient. In particular, the invention concerns encryption of print data in such a manner that the data can only be decrypted using information supplied both by the intended image output device and by the intended recipient.

Description Of The Related Art

In a networked office environment, a print job generated by a computer at one location in the network can be printed by an image output device at another location. If the print job includes confidential or otherwise sensitive information, concerns arise about unauthorized interception of the print job at one of several points in the network. In particular, the print job can be intercepted by a device on the network such as a computer system running simple network snooping tools.

In addition, concerns also arise about unauthorized viewing of the printed output. The printed document may be viewed by any person who happens to be near the image output device before the intended recipient arrives to collect the document.

Similar issues arise with a facsimile transmission. The transmission can be intercepted, and any person who arrives at a destination facsimile machine before the intended recipient can view the facsimile document.

SUMMARY OF THE INVENTION

Accordingly, what is needed is an arrangement whereby a printed or faxed document can only be generated at an intended image output device in the presence of an intended recipient.

The invention addresses the foregoing need by encrypting print data

using a symmetric encryption algorithm with a randomly generated symmetric key, and then encrypting the symmetric key so that it can only be recovered by an intended image output device in the presence of an intended recipient. The encryption of the key is performed by an asymmetric encryption (i.e., public/private key-pair) algorithm. The key is encrypted twice, using public keys for both the intended recipient and for the intended image output device. Then, the encrypted print data and the encrypted randomly generated key are sent to the image output device.

In order to generate an image for the document, the twice-encrypted symmetric key is decrypted using the private keys for both the image output device and the intended recipient. Preferably, the private key for the intended recipient must be personally supplied by the recipient. Upon decryption of the symmetric key, the print data is decrypted using the decrypted symmetric key, and an image is output by the image output device in accordance with the decrypted print data.

As a result of the foregoing arrangement, the symmetric key can only be recovered using the private keys for both the intended recipient and for the intended image output device. Thus, as long as the private keys remain in the sole possession of the intended recipient and the intended image output device, respectively, the symmetric key can only be recovered at the intended image output device in the presence of the intended recipient. Because the symmetric key is needed to decrypt the print data, an image can be printed from the print data only at the intended image output device in the presence of the intended recipient.

Accordingly, one aspect of the present invention concerns secure transmission of data to an intended image output device such as a printer or a facsimile machine. The data can be used to generate an image only at the intended image output device in the presence of an intended recipient. The data is encrypted using a first key. The first key is then tw

ice encrypted using a second key and then a third key. The second key i s the public key of a first private key/public key pair, the private key of the first private key/public key pair being primarily in the sole po ssession of the intended image output device. The third key is the publ ic key of a second private key/public key pair, the private key of the s econd private key/public key pair being primarily in the sole possession of the intended recipient. The encrypted data and the twice-encrypted first key both are then transmitted to the intended image output device.

Preferably, the first key is randomly generated. In addition, the e ncryption of the data with the first key is preferably performed using a symmetric encryption algorithm, and the encryption of the first key wit h the second and third keys are preferably performed using an asymmetric encryption algorithm.

Moreover, the order of encryption of the first key using the second and third keys can be reversed. For instance, encryption of the first k ey using the second key can occur before a second encryption of the firs t key using the third key. Alternatively, encryption of the first key u sing the third key can occur before a second encryption of the first key using the second key.

Preferably, the twice-encrypted first key is contained within a head er along with other information relating to the identities of the sender and the recipient. Also, in the preferred embodiment, the method furth er includes the steps of processing the header and the encrypted data by application of a cryptographic hashing algorithm, resulting in a header hash and a data hash, and of digitally signing the header hash and the data hash with a fourth key. The fourth key is the private key of a thi rd private key/public key pair, the private key of the third private key /public key pair being primarily in the sole possession of the person in itiating the transmission of data. The transmitting step preferably tra

nsmits the signed header hash and the signed data hash along with the en crypted data and the twice-encrypted first key.

By virtue of the foregoing arrangements, data for generating an imag e can be transmitted to an image output device, whereby the image is onl y capable of being printed by the intended image output device in the pr esence of an intended recipient.

In another aspect, the invention concerns generation of an image fro m data transmitted to an intended image output device, such as a printer or a facsimile machine, or such a device itself. The data can be used to generate the image only at the intended image output device in the pr esence of an intended recipient. Encrypted data and a twice-encrypted f irst key are received by the device. The encrypted first key is twice d ecrypted using a second key and a third key, respectively. The second k ey is a private key of a first private key/public key pair, the private key of the first private key/public key pair being primarily in the sole possession of the intended recipient. The third key is a private key o f a second private key/public key pair, the private key of the second pr ivate key/public key pair being primarily in the sole possession of the intended image output device. After the encrypted first key is twice de crypted, the encrypted data is decrypted using the decrypted first key, and an image is generated by the intended image output device from the d ecrypted data.

Preferably, the decryption of the first key using the second and thi rd keys is performed using an asymmetric decryption algorithm. Decrypti on of the encrypted data using the decrypted first key is preferably per formed using a symmetric decryption algorithm.

Depending upon the order of encryption of the first key, decryption of the first key using the second key can occur before decryption of the first key using the third key. Alternatively, decryption of the first

key using the third key can occur before decryption of the first key using the second key.

In the preferred embodiment, the second key is contained in a smart-card which is in the possession of the intended recipient. Thus, the second key is primarily accessible only with permission by the intended recipient. Likewise, the third key is preferably contained in a smart-chip which is maintained internally in the intended image output device, thereby being shielded from access by devices other than the intended image output device.

Preferably, the device also receives a header containing information related to the identities of the sender and the recipient. Also, in the preferred embodiment, the receiving step further includes receipt of a signed header hash and a signed data hash. The authenticity of the signed header hash and of the signed data hash preferably are verified using a fourth key which is the public key of a third public key/private key pair; the private key of the third public key/private key pair being primarily maintained in the sole possession of the person who initiated the transmission of the data for receipt by the device. If the signed header hash or the signed data hash fail verification of authenticity, the encrypted data is preferably discarded. Otherwise, the integrity of the signed header hash and the signed data hash are verified by application of a cryptographic hashing algorithm to the header and the encrypted data. If the signed header hash or the signed data hash fail the verification of integrity, the encrypted data is preferably discarded.

By virtue of the foregoing arrangements, data sent to an image output device is used to generate an image only if the data is intended for that image output device, and only if an intended recipient is present to supply a needed private key.

Another aspect of the invention concerns secure transmission of data

to an intended image output device, wherein the data can be used to gen erate an image only at the intended image output device in the presence of an intended recipient. In this aspect, the data is encrypted twice u sing a first key and a second key, the first key being the public key of a first private key/public key pair, the private key of the first priva te key/public key pair being primarily in the sole possession of the int ended image output device, and the second key being the public key of a second private key/public key pair, the private key of the second privat e key/public key pair being primarily in the sole possession of the inte nded recipient of the image. The twice-encrypted data is then transmitt ed to the intended image output device.

By virtue of the foregoing arrangements, data for generating an imag e can be transmitted to an image output device, whereby the image is onl y capable of being printed by the intended image output device in the pr esence of an intended recipient.

In another aspect, the invention is directed to generation of an ima ge from twice-encrypted data transmitted to an intended image output dev ice, wherein the twice-encrypted data can be used to generate the image only at the intended image output device in the presence of an intended recipient. In this aspect, twice-encrypted data is received and then tw ice decrypted by using a first key and a second key. The first key is th e private key of a first private key/public key pair, the private key of the first private key/public key pair being primarily in the sole posse ssion of the intended recipient of the image. The second key is a priva te key of a second private key/public key pair, the private key of the s econd private key/public key pair being primarily in the sole possession of the intended image output device. An image is then generated from t he decrypted data.

By virtue of the foregoing arrangements, data sent to an image outpu

t device is used to generate an image only if the data is intended for t hat image output device, and only if an intended recipient is present to supply a needed private key.

In yet another aspect of the invention, a method is provided for sec ure transmission of data to an intended image output device, wherein the data can be used to generate an image at the intended image output devi ce in the presence of an intended recipient. The method comprises a fir st encrypting step of encrypting the data using a first key, and a secon d encrypting step of twice encrypting the first key using a second key a nd a third key, the second key being a public key of a first private key /public key pair, a private key of the first private key/public key pair being primarily in the sole possession of the intended image output dev ice, and the third key being a public key of a second private key/public key pair, a private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image . A generating step then generates a header containing the twice-encryp ted first key and in a first transmitting step, the header is transmitte d to the intended image output device. In a receiving step a request is received from the intended image output device for the encrypted data, and then in a second transmitting step the encrypted data is transmitted to the intended image output device.

By virtue of the foregoing arrangements, a header for a print job ca n be sent to an intended image output device, but the corresponding encr ypted data does not have to be sent to the intended image output device until required by the intended image output device. In addition, the in tended image output device is used to generate an image only if the data is intended for that image output device, and only if an intended recip ient is present to supply a needed private key.

In another aspect of the invention, a method is provided for generat

ing an image from data transmitted to an intended image output device, w
herein the data can be used to generate the image at the intended image
output device in the presence of an intended recipient. The method comp
rises a receiving step of receiving a header containing a twice-encrypte
d first key and a sending step of sending a request for encrypted data c
orresponding to the header. The method also comprises a receiving step
of receiving encrypted data corresponding to the header, and a first dec
rypting step of twice decrypting the twice-encrypted first key using a s
econd key and a third key, the second key being a private key of a first
private key/public key pair, the private key of the first private key/p
ublic key pair being primarily in the sole possession of the intended re
cipient of the image, and the third key being a private key of a second
private key/public key pair, the private key of the second private key/p
ublic key pair being primarily in the sole possession of the intended im
age output device. A second decrypting step is provided for decrypting
the encrypted data using the decrypted first key, and an image generatin
g step generates an image from the decrypted data.

By virtue of the foregoing arrangements, a header for a print job ca
n be sent to an intended image output device, but the corresponding encr
ypted data does not have to be sent to the intended image output device
until required by the intended image output device. In addition, the in
tended image output device is used to generate an image only if the data
is intended for that image output device, and only if an intended recip
ient is present to supply a needed private key.

The invention may be implemented in method or apparatus, or computer
-executable process steps, such as a printer driver, an image output dev
ice for transmitting the data for secure printing, as well as special-pu
rpose apparatus such as a printer or a facsimile machine for receiving a
nd printing the data.

This brief summary has been provided so that the nature of the invention may be understood quickly. A more complete understanding of the invention can be obtained by reference to the following detailed description of the preferred embodiments thereof in connection with the attached drawings.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention is generally directed to the secure printing of image data such that the image data can only be printed on an intended output image device in the presence of an intended recipient. The present invention therefore provides a manner by which a document can be securely transmitted from a computer to a remote image output device in a networked environment. The document is maintained in a secure fashion until the intended recipient is present at the intended image output device, whereupon the intended image output device prints the image.

Figure 1 provides an overall system view of a networked computing environment in which the present invention may be implemented. As shown in Figure 1, the networked computing environment comprises a network which is connected to desktop computer 10, laptop computer 20, server 40, digital copier 30 and printer 50. Network 100 is preferably an Ethernet network medium consisting of a bus-type physical architecture, although the invention can be utilized over other types of networks, including the internet.

Desktop computer 10 is preferably an IBM PC-compatible computer having a windowing environment such as Microsoft Windows 95, Windows 98 or Windows NT. As is typical with IBM PC-compatible computers, desktop computer 10 preferably has a display, keyboard, mouse, floppy drive and/or other type of storage medium (not shown). Also attached to desktop computer 10 is smart-card interface device 15 for interfacing with a smart-ca

rd of a computer user, such as smart-card 16. Smart-card 16 therefore p rovides a mechanism whereby a computer user can authenticate the user's identity to desktop computer 10. In addition, smart-card 16 contains a private key of a private/public key pair which is specific to a computer user and which is used in the present invention for the secure printing of image data as discussed more fully below.

Laptop computer 20 is also an IBM PC-compatible computer having a wi ndowing environment such as Microsoft Windows 95, Windows 98 or Windows NT. Like desktop computer 10, laptop computer 20 also has a display, ke yboard, mouse and floppy drive or other storage means (not shown). In a ddition, laptop computer 20 also has a smart-card interface device 25 at tached to it for interfacing to the smart-card of a computer user such a s smart-card 26. Also attached to network 100 is digital copier 30, whi ch is capable of receiving image data over network 100 for printing. Di gital copier 30 also has attached smart-card interface device 35 for int erfacing with the smart-card of a print job recipient, such as smart-car d 36. In addition, server 40 is also connected to network 100. Server 40 preferably comprises an IBM PC-compatible computer having an operatin g system such as DOS, Microsoft Windows 95, Windows 98 or Windows NT, UN IX or other operating system. Server 40 has a storage device 41 which i s preferably a large fixed disk for storing numerous files. Server 40 c an therefore be utilized by other devices on network 100 as a file serve r and may also act as a gateway for other devices on network 100 to anot her network such as the Internet.

Printer 50 is also connected to network 100 and is preferably a lase r or bubble-jet printer which is capable of operating as both a printer and a facsimile device. Printer 50 has a storage device 51 which is pre ferably a large fixed disk, and also has an embedded smart-chip 57 which contains a private key of a private/public key pair corresponding to pr

inter 50 for use in encryption and/or decryption of data received by pri nter 50. In addition, printer 50 is connected to smart-card interface d evice 55 which is capable of interfacing with a smart-card of a print jo b recipient, such as smart-card 56. In this manner, the printing of a p rint job for a particular intended recipient may be controlled through t he use of smart-card interface device 55 and smart-card 56, in combinati on with smart-chip 57 in printer 50.

Figure 2 is a block diagram showing an overview of the internal arch itecture of desktop computer 10. In Figure 2, desktop computer 10 is se en to include central processing unit (CPU) 210 such as a programmable m icroprocessor which is interfaced to computer bus 200. Also coupled to computer bus 200 are keyboard interface 220 for interfacing to a keybar d, mouse interface 230 for interfacing to a pointing device, floppy disk interface 240 for interfacing to a floppy disk, display interface 250 f or interfacing to a display, network interface 260 for interfacing to ne twork 100, and smart-card interface 265 for interfacing to smart-card in terface device 15.

Random access memory ("RAM") 270 interfaces to computer bus 200 to p rovide central processing unit ("CPU") 210 with access to memory storage , thereby acting as the main run-time memory for CPU 210. In particular , when executing stored program instruction sequences, CPU 210 loads the se instruction sequences from fixed disk 280 (or other memory media) int o random access memory ("RAM") 270 and executes those stored program ins truction sequences out of RAM 270. It should also be noted that standar d-disk swapping techniques available under windowing operating systems a llow segments of memory to be swapped to and from RAM 270 and fixed disk 280. Read-only memory ("ROM") 290 stores invariant instruction sequenc es, such as start-up instruction sequences for CPU 210 or basic input/ou tput operation system ("BIOS") sequences for the operation of peripheral

devices attached to computer 10.

Fixed disk 280 is one example of a computer-readable medium that stores program instruction sequences executable by central processing unit ("CPU") 210 so as to constitute operating system 281, printer driver 282, smart-card interface driver 283, other drivers 284, word processing program 285, other programs 286, e-mail program 287 and other files 288. As mentioned above, operating system 281 is preferably a windowing operating system, although other types of operating systems may be used with the present invention. Printer driver 282 is utilized to prepare image data for printing on at least one image output device, such as printer 50. Smart-card interface driver 283 is utilized to drive and control smart-card interface 265 for interfacing with smart-card interface device 15 so as to read and write to a smart-card such as smart-card 16. Other drivers 284 include drivers for each of the remaining interfaces which are coupled to computer bus 200.

Word processing program 285 is a typical word processor program for creating documents and images, such as Microsoft Word, or Corel WordPerfect. Other programs 286 contains other programs necessary to operate desktop computer 10 and to run desired applications. E-mail program 287 is a typical e-mail program that allows desktop computer 10 to receive and send e-mails over network 100. Other files 288 include any of the files necessary for the operation of desktop computer 10 or files created and/or maintained by other application programs on desktop computer 10.

Figure 3 is a block diagram showing an overview of the internal architecture of printer 50. In Figure 3, printer 50 is seen to contain a printer smart-chip 57 which, as previously mentioned, contains a private key corresponding to printer 50 for encryption/decryption purposes. Printer 50 also contains a central processing unit ("CPU") 310 such as a programmable microprocessor which is interfaced to printer bus 300. Also c

oupled to printer bus 300 are control logic 320, which is utilized to co ntrol the printer engine of printer 50 (not shown), I/O ports 330 which is used to communicate with various input/output devices of printer 50 (not shown), smart-card interface 365 which is utilized to interface with smart-card interface device 55, and network interface 360 which is util ized to interface printer 50 to network 100.

Also coupled to printer bus 300 are EEPROM 340, for containing non-v olatile program instructions, random access memory ("RAM") 370, printer memory 51 and read-only memory ("ROM") 390. RAM 370 interfaces to print er bus 300 to provide CPU 310 with access to memory storage, thereby act ing as the main run-time memory for CPU 310. In particular, when execut ing stored program instruction sequences, CPU 310 loads those instructio n sequences from printer memory 51 (or other memory media) into RAM 370 and executes those stored program instruction sequences out of RAM 370. ROM 390 stores invariant instruction sequences, such as start-up instru ction sequences for CPU 310 or BIOS sequences for the operation of vario us peripheral devices of printer 50 (not shown).

Printer memory 51 is one example of a computer-readable medium that stores program instruction sequences executable by CPU 310 so as to cons titute printer engine logic 351, control logic driver 352, I/O port driv ers 353, smart-card interface driver 354, encryption/decryption logic 35 5, queue 356, other files 357, printer smart-chip driver 358, and e-mail program 359. Printer engine logic 351 and control logic driver 352 are utilized to control and drive the printer engine of printer 50 (not sho wn) so as to print an image according to image data received by printer 50, preferably over network 100. I/O port drivers 353 are utilized to d rive the input and output devices (not shown) connected through I/O port s 330. Smart-card interface driver 354 is utilized to drive smart-card interface 365 for interfacing to smart-card interface device 55, thereby

enabling printer 50 to read and write to a smart-card such as smart-card 56.

Encryption/decryption logic 355 enables printer 50 to receive encrypted data according to the present invention and to carry out the necessary steps to enable the decryption of the encrypted print data in the presence of an intended recipient. The details of these steps are discussed more fully below. Queue 356 is utilized to contain a print queue comprised of numerous print jobs which are to be printed. Other files 357 contain other files and/or programs for the operation of printer 50. Printer smart-chip driver 358 is utilized to drive and interface with printer smart-chip 57 for encryption/decryption purposes. Lastly, e-mail program 359 is a typical e-mail program for enabling printer 50 to receive e-mail messages from network 100. Such e-mail messages may contain print job-related information, as discussed in more detail below.

Figure 4 is a block diagram showing an overview of the internal architecture of server 40. In Figure 4, server 40 is seen to include a central processing unit ("CPU") 410 such as a programmable microprocessor which is interfaced to computer bus 400. Also coupled to computer bus 400 is a network interface 460 for interfacing to network 100. In addition, random access memory ("RAM") 470, fixed disk 41, and read-only ("ROM") 490 are also coupled to computer bus 400. RAM 470 interfaces to computer bus 400 to provide CPU 410 with access to memory storage, thereby acting as the main run-time memory for CPU 410. In particular, when executing stored program instruction sequences, CPU 410 loads those instruction sequences from fixed disk 41 (or other memory media) into RAM 470 and executes those stored program instruction sequences out of RAM 470. It should also be recognized that standard disk-swapping techniques allow segments of memory to be swapped to and from RAM 470 and fixed disk 41. ROM 490 stores invariant instruction sequences, such as start-up instruc

tion sequences for CPU 410 or basic input/output operating system ("BIOS") sequences for the operation of peripheral devices which may be attached to server 40 (not shown).

Fixed disk 41 is one example of a computer-readable medium that stores program instruction sequences executable by CPU 410 so as to constitute operating system 411, network interface driver 412, encryption/decryption logic 413, e-mail program 414, queue 415, and other files 416. As mentioned above, operating system 411 can be an operating system such as DOS, Windows 95, Windows 98, Windows NT, UNIX, or other such operating system. Network interface driver 412 is utilized to drive network interface 460 for interfacing server 40 to network 100. Encryption/decryption logic 413 allows server 40 to receive encrypted data and to either maintain such data in queue 415 or to send such data to an image output device such as printer 50 for printing. E-mail program 414 is a typical e-mail program and enables server 40 to receive and/or send e-mail messages over network 100. Queue 415 is utilized to store numerous print jobs for output on one or more image output devices, such as printer 50. Lastly, other files 416 contains other files or programs necessary to operate server 40 and/or to provide additional functionality to server 40.

Figure 5A is a view for explaining the encryption process of the present invention which enables a computer user of a computer on network 100, such as desktop computer 10, to send data related to a print job for printing only on an intended image output device when an intended recipient is present. For instance, a computer user located at desktop computer 10 may wish to prepare a document using word processing program 285 for printing only on printer 50 at a later time when an intended recipient is physically present at printer 50. Most importantly, the computer user at desktop computer 10 wishes to protect the print job data from being accessed or viewed by any device other than printer 50 or by any pers

on other than the intended recipient. Therefore, the present invention encrypts the image data so that it cannot be accessed by any other computer user or device on network 100 and so that it will remain encrypted up until the time the intended recipient is physically present at the intended printer. In this manner, even if the encrypted data is accessed at any point prior to the printing on the intended printer 50, the data will only appear to be a pile of unintelligible bits.

Specifically, as seen in Figure 5A, the encryption process starts with image data 501 which is preferably created by a computer user at desktop computer 10 using a program such as word processing program 285. When the computer user is ready to send a print job corresponding to data 501 to an intended printer, such as printer 50, for receipt by an intended recipient, the user preferably presses a button provided in word processing program 285 to indicate that the document is to be printed in a secure fashion. In the preferred mode, printer driver 282 handles the encryption process for encrypting data 501 before it is sent over network 100 to printer 50. Preferably, printer driver 282 generates a randomly-generated symmetric key for use with a symmetric encryption algorithm.. Data 501 is then encrypted by applying the symmetric encryption algorithm using the randomly-generated symmetric key 510, thereby creating symmetrically encrypted data 502. In this manner, symmetrically encrypted data 502 can only be decrypted by a device having a similar symmetric encryption algorithm and a copy of symmetric key 510. Therefore, symmetric key 510 and symmetrically encrypted data 502 must be passed to printer 50 in order for the data to eventually be decrypted and printed out for the intended recipient. In order to maintain security until such time as data 501 is printed on printer 50, symmetric key 510 is also encrypted with two public keys which correspond to the intended printer and the intended recipient. Each public key is from a public key/private key pair

which is used in an asymmetric encryption algorithm. In this manner, o nly the combination of private keys of the intended recipient and the in tended printer will allow symmetric key 510 to be decrypted such that sy mmetrically encrypted data 502 can be decrypted for printing.

Therefore, as seen in Figure 5A, printer public key 520 correspondin g to printer 50 is obtained from a public key infrastructure which is pr ovided on a server on network 100, from a third-party key service via ne twork 100, or from another suitable source such as a local key storage f ile. Printer public key 520 is then utilized in conjunction with an asy mmetric encryption algorithm to encrypt symmetric key 510, thereby creat ing printer-key-encrypted symmetric key 511. In this manner, symmetric key 510 cannot be accessed without the corresponding private key of the public/private key pair corresponding to printer 50. As discussed above , the private key for printer 50 is preferably maintained in smart-chip 57 which is embedded within printer 50 so as to prevent exposure of the private key to any other person or device. In this manner, printer key encrypted symmetric key 511 can only be decrypted by the intended image output device, in this case printer 50.

Although the above encryption of symmetric key 510 ensures that only the intended printer can print the print job, it does not ensure that o nly the intended recipient will receive the print job for viewing. Ther efore, it is also preferable to further encrypt symmetric key 510 with a public key corresponding to the intended recipient. As shown in Figure 5A, recipient public key 530 is also obtained from a public key infrast ructure, or other suitable source. The printer-key-encrypted symmetric key 511 is then encrypted again using recipient public key 530 in conjun ction with an asymmetric encryption algorithm to create twice-encrypted symmetric key 512. Twice-encrypted symmetric key 512 is shown to be enc rypted at a first layer with printer public key 520 and at a second laye

r with recipient public key 530, thereby preventing access to symmetric key 510 unless the specific combination of private keys of the intended recipient and intended printer is provided.

As further shown in Figure 5A, a header 540 is provided to contain t wice-encrypted symmetric key 512 and also to contain information related to the print job such as the sender's identity, the intended recipient's identity, and other information such as the size of the print job, and printer-related settings such as selection of a collating option, a stapling option, and a paper-selection option. In this manner, non-confidential information related to the print job itself can be provided to the intended printer for purposes of print job queuing and identification of the print job for eventual printing. It can be appreciated that header 540 may contain other types of information and may also be provided in a format which does not contain twice-encrypted symmetric key 512. In the preferred embodiment, header information 540 is prepended to twice-encrypted symmetric key 512 to create header 551. Once header 551 is created, an integrity algorithm is applied to header 551 and symmetrically encrypted data 502 in order to provide an integrity check whereby the receiving device may verify that header 551 and symmetrically encrypted data 502 have not been altered in any fashion. Specifically, header 551 and symmetrically encrypted data 502 are processed with hash algorithm 570 which is used to ensure the integrity of the data. The algorithm results in a value known as a "hash" which represents a type of checksum for the corresponding data.

Therefore, a data hash 553 and a header hash 554 are created and are thereupon digitally signed using sender private key 560 of a private key/public key pair corresponding to the sender who initiated the print job. In this manner, print job 550 is created which contains header 551, symmetrically encrypted data 502, data hash 553 and header hash 554. Se

oder private key 560 is preferably obtained from a smart-card, such as s mart-card 16, belonging to the sender at desktop computer 10 via smart-c ard interface device 15. In the case where the sender and the intended recipient are the same person, sender private key 560 is from the same p rivate key/public key pair as the recipient public key 530. In such a s ituation, the sender can send a secure print job to an intended printer from a remote location and can then later retrieve the print job with th e sender's smart-card at the printer.

In this manner, print job 550 can be transmitted to the intended ima ge output device, in this case printer 50, for being queued and eventual ly printed in the presence of the intended recipient. Intended printer 50 can then perform authentication of the sender of print job 550, verif ication of the integrity of header 551 and encrypted data 502 of print j ob 550, decryption of twice-encrypted symmetric key 512, and, finally, d ecryption of encrypted data 502 for printing on printer 50.

The encryption arrangement provided in Figure 5A is a preferred embo diment of the present invention; however, it can be appreciated that the data corresponding to a secure print job can be encrypted using other c ombinations of public keys, and can also be encrypted directly using the aforementioned public keys with an asymmetric encryption algorithm. Fo r instance, the order of encryption of symmetric key 510 can be reversed such that symmetric key 510 is first encrypted using recipient public k ey 530 and is then encrypted using printer public key 520. Therefore, t wice-encrypted symmetric key 512 would first be decrypted using the priv ate key of the intended printer and would then be decrypted using the pr ivate key of the intended recipient.

In Figure 5B, the data associated with the secure print job is twice -encrypted using the public keys of the intended printer and intended re cipient in conjunction with an asymmetric encryption algorithm. Instead

of with a symmetric key as shown in Figure 5A. In Figure 5B, data 581 is the print data associated with the secure print job. As in Figure 5A, public keys of the intended printer (520) and intended recipient (530) are first obtained from a public key infrastructure or other suitable source. Thereafter, data 581 is encrypted using an asymmetric encryption algorithm in conjunction with recipient public key 530 so as to create recipient-key-encrypted data 582. Then, recipient-key-encrypted data 582 is again encrypted using an asymmetric encryption algorithm in conjunction with printer public key 520 to create twice-encrypted data 583. Therefore, as shown in Figure 5B, the data itself is twice-encrypted for transmission to the intended printer after which it can only be decrypted with the private keys of the intended printer and the intended recipient, respectively.

Thus, the encryption arrangement depicted in Figure 5B may be utilized to provide secure printing of a document ordinarily without the use of a symmetric key as depicted in Figure 5A. The arrangement in Figure 5B may also be combined with the other features of Figure 5A, such as the creation of a header and a signed hash prior to transmittal of the twice-encrypted data to the intended printer. It should be noted that the encryption arrangement of Figure 5A is the preferred embodiment because double-encryption of a potentially large amount of data corresponding to data 581 as depicted in Figure 5B may require substantially greater computing resources than the encryption arrangement of Figure 5A wherein only symmetric key 510 is double-encrypted.

Figure 5C is a view for explaining the decryption and printing of data 501 which was encrypted according to Figure 5A. First, print job 550 is received at the intended printer, in this case printer 50, via network 100, and contains the same components as depicted in Figure 5A. Next, sender public key 561 is preferably obtained from a public key infrast

ructure, or other suitable source, and corresponds to the computer user at desktop computer 10 who sent the print job to printer 50. In the alternative, sender public key 561 can be provided in a copy of the sender's digital certificate contained within header information 540. Sender public key 561 is then used in conjunction with hashing algorithm 570 to authenticate and verify the integrity of header 551 and symmetrically encrypted data 502. Specifically, signed header hash 554 and signed data hash 553 are authenticated using sender public key 561 to verify that the sender was indeed the creator of print job 550. If the authentication fails, the print job is preferably discarded.

Next, print job 550 is stored in queue 356 of printer 50 or, in the alternative, is stored in queue 415 of server 40 for subsequent access by printer 50. Once the intended recipient is physically present at printer 50, recipient private key 531 is obtained through the recipient's smart-card, such as smart-card 56, which is inserted into smart-card interface device 55. For security reasons, recipient private key 531 is maintained solely on smart-card 56 and cannot be read by printer 50. Therefore, twice-encrypted symmetric key 512 is passed from printer 50 to smart-card 56 via smart-card interface device 55 where it is partially decrypted using recipient private key 531. Thereafter, partially-decrypted symmetric key 511 is returned from smart-card 56 to printer 50, wherein it is completely decrypted within smart-chip 57 of printer 50. This results in a "clear text" form of symmetric key 510.

Symmetric key 510 is then utilized to decrypt symmetrically-encrypted data 502 in order to obtain a clear text form of data 501. An image is then printed on printer 50 based upon decrypted data 501. In this manner it can be seen that the present invention provides the ability to transmit a document or image to an intended printer for printing only in the presence of an intended recipient. Until the intended recipient's pr

csence is verified at the location of the intended printer, the print jo b is maintained in an encrypted form and cannot reasonably be decrypted by any other person or device that may have intercepted the encrypted da ta.

Figure 5D is a view for explaining the decryption and printing of tw ice-encrypted print data 583 which was encrypted pursuant to the alterna tive of Figure 5B. First, twice-encrypted data 583 is passed to smart-c ard 56 of the intended recipient via smart-card interface 55, whereupon twice-encrypted data 583 is partially decrypted by using recipient priva te key 531 which is located in smart-card 56. Smart-card 56 thereupon r eturns the now partially-decrypted data 582 back to the control of print er 50. Next, partially-decrypted data 582 is passed to smart-chip 57 of printer 50 where partially-encrypted data 582 is completely decrypted u sing printer private key 521 contained in smart-chip 57 in printer 50. The decrypted, "clear" data 581 is now returned from smart-chip 57 to pr inter 50 for printing.

Although the encryption/decryption described in Figures 5B and 5D pr ovide secure printing to an intended printer for an intended recipient, it can be seen that substantially greater resources may be required by s mart-chip 57 and smart-card 56 to process twice-encrypted data in compar ison to the resources required to process a twice-encrypted symmetric ke y as depicted in Figures 5A and 5C. Other collateral features depicted in Figure 5B, such as authentication and integrity verification, may als o be incorporated in the decryption process of Figure 5D.

The hashing process depicted in Figure 5A provides signed data hash 553 which is a type of checksum that allows the receiving device, such a s printer 50, to verify the integrity of the symmetrically encrypted dat a 502. Figure 6 shows a view for explaining one method of generating an d formatting a signed hash for the data. In Figure 6, print data 601, w

hich corresponds to the image to be securely printed, is in an unencrypted, "plaintext" format. A hashing algorithm, which is preferably a one-way hash function, is then applied to print data 601 to create data hash 610 which is essentially a message digest. Data hash 610 is then digitally signed using the private key of the sender, such as sender private key 560 of Figure 5A. Signed hash 611 may then be optionally encrypted. In either case, signed hash 611 is copied to signed hash 612 which is part of data block 600 for transmission to the intended printer where it is used for authentication and integrity verification purposes.

Figure 7A is a view for explaining the structure of the header according to a preferred embodiment of the invention. Specifically, recipient ID 701, sender ID 702 and symmetric key 703 are initially provided in a clear, plaintext format for inclusion in header 700 as depicted in Figure 7A. A hashing algorithm is then collectively performed on recipient ID 701, sender ID 702 and symmetric key 703 to create hash 720. Hash 720 is then signed with the private key of the sender, such as sender private key 560 as depicted in Figure 5A, to create signed hash 721. Signed hash 721 may then be optionally encrypted. In either case, signed hash 721 is then copied to signed hash 722 for inclusion in header 700.

Recipient ID 701 is left in a clear, plaintext format, copied to recipient ID 711 and included in header 700. In the alternative, recipient ID 701 may be encrypted with the public key of the intended printer for anonymity of the intended recipient's identification, copied to recipient ID 711 and included in header 700. In either case, the intended printer can extract and read recipient ID 711 upon receipt of the header, thereby allowing the intended printer to queue the print job corresponding to the intended recipient. Sender ID 702 may be encrypted with the public key of the intended printer before inclusion in header 700, but such encryption is not necessary. Either way, sender ID 702 is copied to se

nder ID 712 and included in header 700. Symmetric key 703 is preferably twice-encrypted as shown in Figure 5A and then provided in twice-encrypted, symmetric key 713 and included in header 700.

An alternative structure for the header is shown in Figure 7B whereby the header is structured so that it can be transmitted to the intended printer separately from the encrypted data. Specifically, recipient ID 751, sender ID 752, symmetric key 753 and a uniform resource locater (URL) 754 are initially provided in a clear, plaintext format for inclusion in header 750 as depicted in Figure 7A. URL 754 is preferably an address location where the encrypted data is stored for later retrieval and transmission to the intended printer. For instance, twice-encrypted data 512, as depicted in Figure 5A, would be maintained on fixed disk 280 of desktop computer 10, or on fixed disk 41 of server 40, at a memory location corresponding to URL 754. URL 754 is then included in header 750 which is sent to the intended printer without the encrypted data that corresponds to header 750. Desktop computer 10, or server 40, as the case may be, subsequently sends the corresponding encrypted data to the intended printer upon receipt of a request from the intended printer which contains a reference to URL 754. In this manner, the intended printer does not use memory space for storing the encrypted data until it is needed, upon which the intended printer pulls the encrypted data from its storage location by reference to corresponding URL 754.

A hashing algorithm is collectively performed on recipient ID 751, sender ID 752, symmetric key 753 and URL 754 to create hash 770. Hash 770 is then signed with the private key of the sender, such as sender private key 560 as depicted in Figure 5A, to create signed hash 771. Signed hash 771 may also be optionally encrypted for further security. In either case, signed hash 771 is copied to signed hash 772 for inclusion in header 750.

Recipient ID 751 is left in a clear, plaintext format, copied to recipient ID 761 and included in header 750. In the alternative, recipient ID 751 may be encrypted with the public key of the intended printer for anonymity of the intended recipient's identification, copied to recipient ID 761 and included in header 750. In either case, the intended printer can extract and read recipient ID 761 upon receipt of the header, thereby allowing the intended printer to queue the print job corresponding to the intended recipient. Sender ID 752 may be encrypted with the public key of the intended printer before inclusion in header 750, but such encryption is not necessary. Either way, sender ID 752 is copied to sender ID 762 and included in header 750. Symmetric key 753 is preferably twice-encrypted pursuant to the method shown in Figure 5A and is then provided as twice-encrypted, symmetric key 763 and included in header 750. In this alternative header format, URL 754 is also encrypted, either with the public key of the intended printer or with symmetric key 753, and then stored in URL 764 in header 750.

By this arrangement, header 750 can then be transmitted separately to the intended printer prior to the transmission of the encrypted data, corresponding to header 750. In this embodiment of the invention, header 750 is preferably transmitted via an E-mail message to the intended printer, such as printer 50, through E-mail program 287 of desktop computer 10 for receipt by E-mail program 359 of printer 50. Other means of sending header 750 over network 100 to printer 50 can also be used, such as through the use of one or more network protocols. When the encrypted data is needed by printer 50, such as when the intended recipient is present at printer 50, printer 50 can decrypt URL 754 and send a data request containing a reference to URL 754. The encrypted data corresponding to URL 754 is then sent to the intended printer for decryption and printing. Symmetric key 763 is then preferably decrypted in the manner descri

bed in Figure 5C, after which the encrypted data is decrypted and printe d in the presence of the intended recipient. In this manner, the memory capacity of the intended printer or of a file server utilized by the in tended printer is not burdened with large files of encrypted print data until it is necessary to retrieve such print data for decryption and pri nting.

Figure 8 is a flowchart for explaining the overall encryption and tr ansmission of a secure print job according to a preferred embodiment of the present invention. The process steps shown in this figure, as well as those of Figure 9, are computer-executable process steps stored on a computer-readable memory medium such as disk 280, disk 41, or printer me mory 51. First, in step S801, a sender working on a computer in a netwo rked computing environment submits a print job for sending a document or image for secure printing at an intended image output device, such as a printer or facsimile device, in the presence of an intended recipient. Preferably, the print job is submitted by pressing a button in a word p rocessing application, such as Microsoft Word, whereupon a printer drive r interface appears for collecting necessary information, such as the in tended recipient, and the like. In the alternative, a separate client a pplication may be provided to collect such information. Preferably, the printer driver also performs the remaining steps of Figure 8 for encryp tion and transmittal of a secure print job.

Next, the image data associated with the print job is encrypted with a randomly-generated symmetric key in conjunction with a symmetric encr yption algorithm as discussed above with regard to Figure 5A (step S802) . In step S803, the public key for the intended recipient and for the i ntended printer, respectively, are obtained from a public key infrastruc ture, or other suitable source, and the sender's private key is obtained , preferably from a smart-card 16 belonging to the sender via smart-card

interface device 15. In step S804, the symmetric key is twice encrypte d, by first encrypting the symmetric key with the public key of the inte nded printer in conjunction with an asymmetric encryption algorithm, and then encrypting the symmetric key again with the public key of the inte nded recipient in conjunction with an asymmetric encryption algorithm.

After the symmetric key is twice-encrypted, a header is formed which includes the twice-encrypted symmetric key and which also includes info rmation related to the print job such as the identity of the intended re cipient and of the sender in an unencrypted format (step S805). As disc ussed above, the header may also include a URL which points to the locat ion of the encrypted data which corresponds to the header in the case wh ere the header is to be sent separately from the encrypted data. In ste p S806, a hashing algorithm is then applied to the header to form a head er hash and to the encrypted data to form a data hash. The header hash and data hash are then digitally signed with the private key of the send er in step S807. The header hash and data hash may also be optionally e ncrypted for additional security. Preferably, the private key of the se nder is obtained from a smart-card which is kept in the possession of th e sender. In the alternative, a token, flashrom or other means of stora ge can be used to securely store the private key of the sender.

Next, it is determined in step S808 whether the header is to be sent to the intended printer separate from the corresponding encrypted data. If the header is to be sent separately, control passes to step S809 i n which the print job, comprising the header and the header hash, is sen t over the network to the intended printer without the corresponding enc rypted data. Preferably, the intended printer has an E-mail program and the print job containing the header and header hash is sent to the prin ter by means of E-mail, although the print job may be separately sent to the intended printer by other means, such as via one or more other netw

ork protocols. In the preferred mode, the header contains a URL which c orresponds to the location in memory of the encrypted data and data hash . This location can reside on a disk of a computer or server which is a ccessible by the intended printer via the network. The corresponding en crypted data and data hash are then subsequently sent to the intended pr inter by the server or computer on which the encrypted data and data has h are stored in step S810, either automatically or at the request of the intended printer by reference to the URL which was provided to the inte nded printer in the earlier received header. Control then passes to the end (step S812).

If, however, it is determined in step S808 that the header is not to be sent separately from the corresponding encrypted data to the intende d printer, control is passed to step S811 in which a print job comprisin g the header, header hash, encrypted data, and data hash are transmitted over the network to the intended printer. Control then passes to the e nd in step S812. In this embodiment, the intended printer receives the encrypted data along with the header which contains the twice-encrypted symmetric key for decryption of the encrypted data. In addition, the he ader hash and data hash are received by the intended printer for verific ation of the authenticity and integrity of the header and encrypted data .

Figure 9 is a flowchart for explaining the decryption and printing o f a secure print job according to a preferred embodiment of the present invention. First, the intended printer receives a secure print job in s tep S901. As discussed above with respect to Figure 8, the print job ma y only comprise the header and header hash as in the case where the head er and header hash are received by the intended printer separately by E-mail. Otherwise, the print job comprises the encrypted data and data ha sh along with the header and header hash and is received by the intended

printer by normal means over the network.

Next, the public key of the sender is obtained from a public key infrastructure, from another suitable source, or from a copy of the sender's digital certificate provided in the header for use in the subsequent authentication and verification of integrity of the secure print job (step S902). In step S903 the sender's public key is used to check the authenticity of the digital signature of the header hash of the secure print job. If the header hash is not authentic, control passes to step S904 in which a notice is preferably sent to the sender to warn the sender that a non-authenticated print job has been detected. Next, in step S905 the print job is discarded. Flow then passes to the end in step S919. If, however, the header hash is determined to be authentic in step S903, flow passes to step S906 in which the integrity of the header is verified against the header hash.

In step S906 a hashing algorithm is used to compare the header to the signed data hash to verify that the header was received intact and was not tampered with, therefore indicating that the header is of reliable integrity. If the integrity of the header is in question, control passes to step S905 in which the print job is discarded. Control then passes to the end in step S919. If, however, the header is of reliable integrity, control passes to step S907 in which header information, such as the identity of the intended recipient, is extracted from the header whereupon the print job is placed in a print queue for subsequent printing. Preferably, the print job is sent from the printer to a local server on the network where it is stored in a print queue according to the identification of the intended recipient until subsequently retrieval by the intended printer. In the alternative, the print queue may be maintained in a large memory device within the intended printer itself.

In step S908, the intended recipient arrives at the location of the

intended printer and inserts a smart-card belonging to the intended recipient into a smart-card interface device which is connected to the intended printer. Preferably, the smart-card contains a unique private key and also contains authenticating identification information corresponding to the intended recipient. The printer, via the smart-card interface device, obtains the authenticating identification information of the intended recipient from the smart-card and determined whether the identification of the intended recipient is authentic (step S909). If the identification information is not authentic, control passes to the end in step S919. If the identification information is authentic, the print queue, which is located in either the printer itself or in a local server, is queried, preferably by reference to the identification of the intended recipient, to determine if there are any print jobs corresponding to the intended recipient (step S910). If there are not any print jobs in the print queue corresponding to the intended recipient, control passes to the end in step S919. If, on the other hand, there is a print job in the print queue corresponding to the intended recipient, the next sequential print job in the print queue is obtained and control passes to step S911.

In step S911, the print job is examined to determine if the print job contains only the header and header hash, as in the case where the header and header hash are sent separately by e-mail to the printer without the encrypted data and data hash. If this is the case, the intended printer sends a request to the location where the encrypted data is stored, such as a server or computer on the network, to retrieve the encrypted data whereupon the encrypted data and corresponding data hash are transmitted from the server or computer, as the case may be, to the intended printer (step S912). In the preferred mode, the request by the intended printer to retrieve the encrypted data contains a reference to a URL co

ntained in the header which was received earlier by the intended printer , wherein the URL points to the location of the encrypted data and corresponding data hash. In this manner, the intended printer is not required to store large files of encrypted data until they are needed for printing, at which time the encrypted data is pulled from its location on a server or computer to the intended printer. The retrieval request by the printer and subsequent transmission of the encrypted data and data hash preferably are implemented by normal network communication means, such as TCP/IP protocol and HTTP protocol where the retrieval request contains a reference to a URL, although other protocols such as FTP may also be used. Control then passes to step S913. If it is determined in step S911 that the header was not sent separately to the intended printer, then the print job already comprises the encrypted data along with the header, and therefore control passes directly to step S913.

Next, in step S913, the twice-encrypted symmetrical key is extracted from the header of the print job and is partially decrypted by using the private key of the intended recipient in conjunction with an asymmetric decryption algorithm. In the preferred embodiment, the smart-card of the intended recipient contains the intended recipient's private key and also contains a microprocessor such that the twice-encrypted symmetrical key is passed to the smart-card by the printer through a smart-card interface device. In this manner, the partial decryption actually takes place on the smart-card itself, thereby preventing external access to the private key of the intended recipient which is contained on the smart-card.

The partially decrypted symmetric key is then returned from the smart-card to the printer whereupon the partially decrypted symmetric key is completely decrypted by using the private key of the intended printer in conjunction with an asymmetric decryption algorithm (step S914). Pref

erably, the private key of the intended printer is contained in a smart-chip which is embedded within the printer. The partially decrypted symmetric key is passed to the smart-chip where it is completely decrypted using the private key contained in the smart-chip, thereby preventing external access to the printer's private key which is contained on the smart-chip. Other means for storing the private key of the intended printer could also be used, such as a token, flashrom, or the like.

The completely decrypted, "clear" symmetric key is then returned from the smart-chip to the intended printer, whereupon the decrypted, "clear" symmetric key is used to decrypt the encrypted data pursuant to a symmetric decryption algorithm (step S915). Next, the integrity of the decrypted data is verified in step S916 by comparing the data with the data hash through the use of a hashing algorithm as discussed above. If the integrity of the decrypted data cannot be verified, then the data may have been intercepted and/or tampered with such that it cannot be relied upon, and therefore control is passed to step S917 in which the entire print job is discarded. Control is then passed to the end in step S919. If, however, the integrity of the decrypted data is verified in step S916, control passes to step S918 in which an image is printed by the intended printer in accordance with the decrypted data (step S912). Control then passes to the end in step S919.

In this manner, secure printing is provided such that an image can be generated only by an intended image output device in the presence of an intended recipient. In particular, the print data is encrypted in such a manner that the data can only be decrypted using a combination of secret keys which are supplied by the intended image output device and by the intended recipient, respectively.

The invention has been described with particular illustrative embodiments. It is to be understood that the invention is not limited to the

above-described embodiments and that various changes and modifications m ay be made by those of ordinary skill in the art without departing from the spirit and scope of the invention.

4. Brief description of the drawings

Figure 1 is a representative view of a networked computing environme nt in which the present invention may be implemented.

Figure 2 is a detailed block diagram showing the internal architectu re of the computer shown in Figure 1 according to the present invention.

Figure 3 is a detailed block diagram showing the internal architectu re of the printer shown in Figure 1 according to the present invention.

Figure 4 is a detailed block diagram showing the server shown in Fig ure 1 according to the present invention.

Figure 5A is a view for providing an explanation of encryption of da ta and a symmetric key of a secure print job according to a first embodi ment of the present invention.

Figure 5B is a view for providing an explanation of encryption of da ta of a secure print job according to a second embodiment of the present invention.

Figure 5C is a view for providing an explanation of the decryption a nd printing of a secure print job according to an embodiment of the pres ent invention.

Figure 5D is a view for providing an explanation of the decryption a nd printing of a secure print job according to another embodiment of the present invention.

Figure 6 is a view for providing an explanation of the structure of an encrypted data format according to an embodiment of the present inven tion.

Figure 7A is a view for providing an explanation of the structure of

an encrypted header format according to an embodiment of the present in vention.

Figure 7B is a view for providing an explanation of the structure of an encrypted header format according to another embodiment of the prese nt invention.

Figure 8 is a flowchart for providing an explanation of encryption a nd transmission of a secure print job according to the present invention .

Figure 9 is a flowchart for providing an explanation of decryption a nd printing of a secure print job according to the present invention.

【図１】

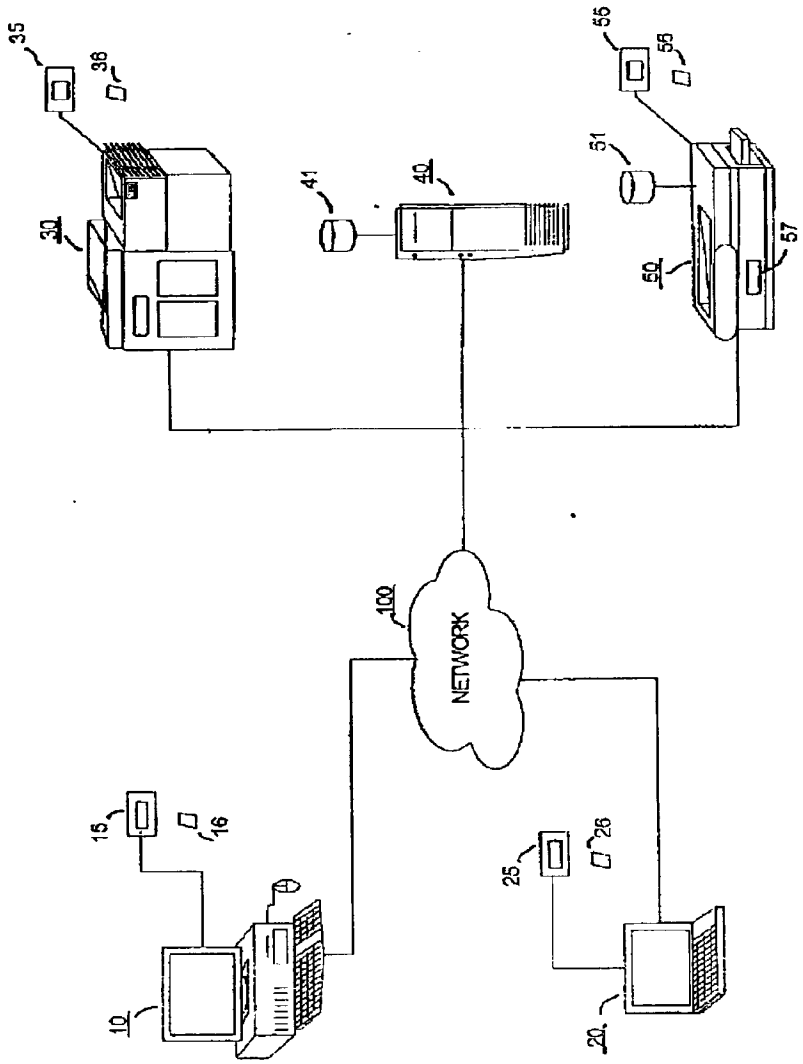


FIG. 1

【図２】

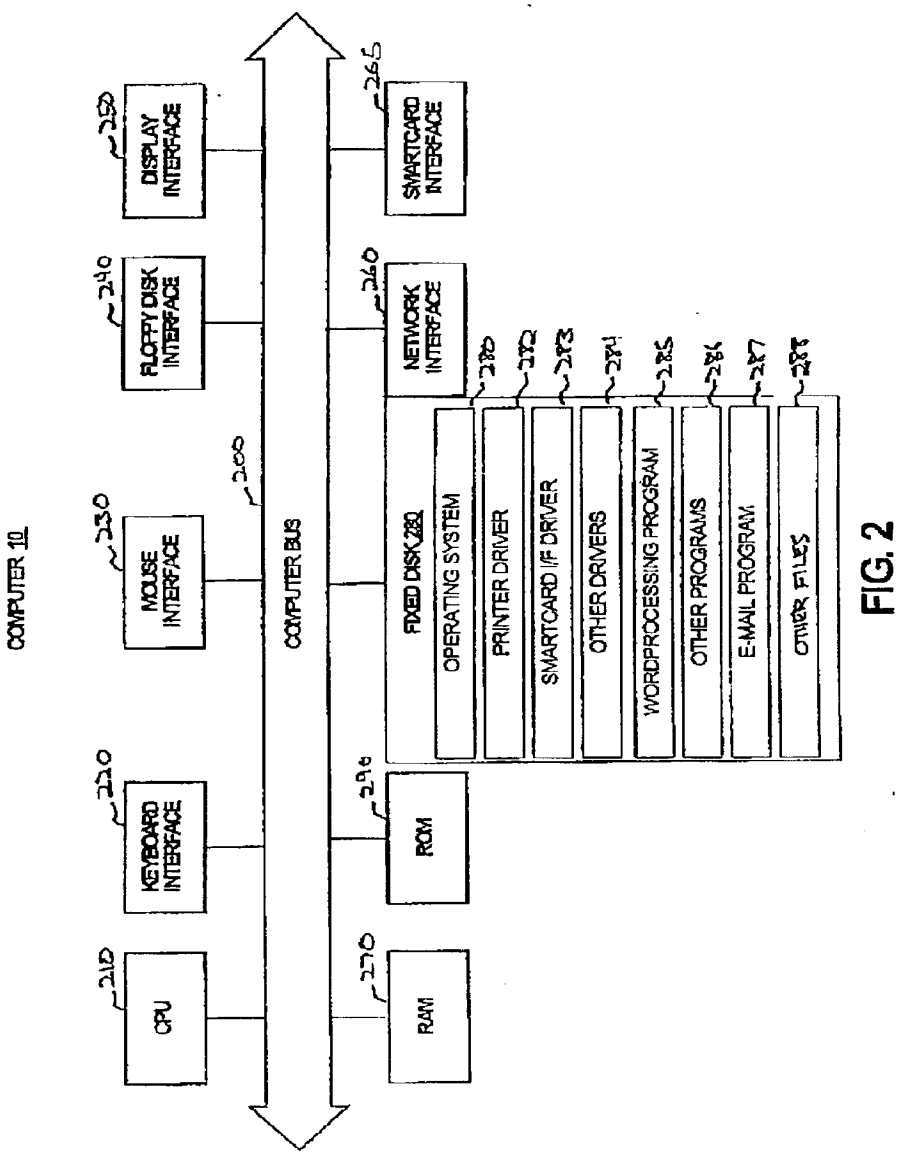

COMPUTER 10
COMPUTER BUS
DISPLAY INTERFACE
FLOPPY DISK INTERFACE
MOUSE INTERFACE
KEYBOARD INTERFACE
CPU
SMARTCARD INTERFACE
NETWORK INTERFACE
FIXED DISK
OPERATING SYSTEM
PRINTER DRIVER
SMARTCARD I/F DRIVER
OTHER DRIVERS
WORDPROCESSING PROGRAM
OTHER PROGRAMS
E-MAIL PROGRAM
OTHER FILES
ROM
RAM

FIG. 2

【図３】

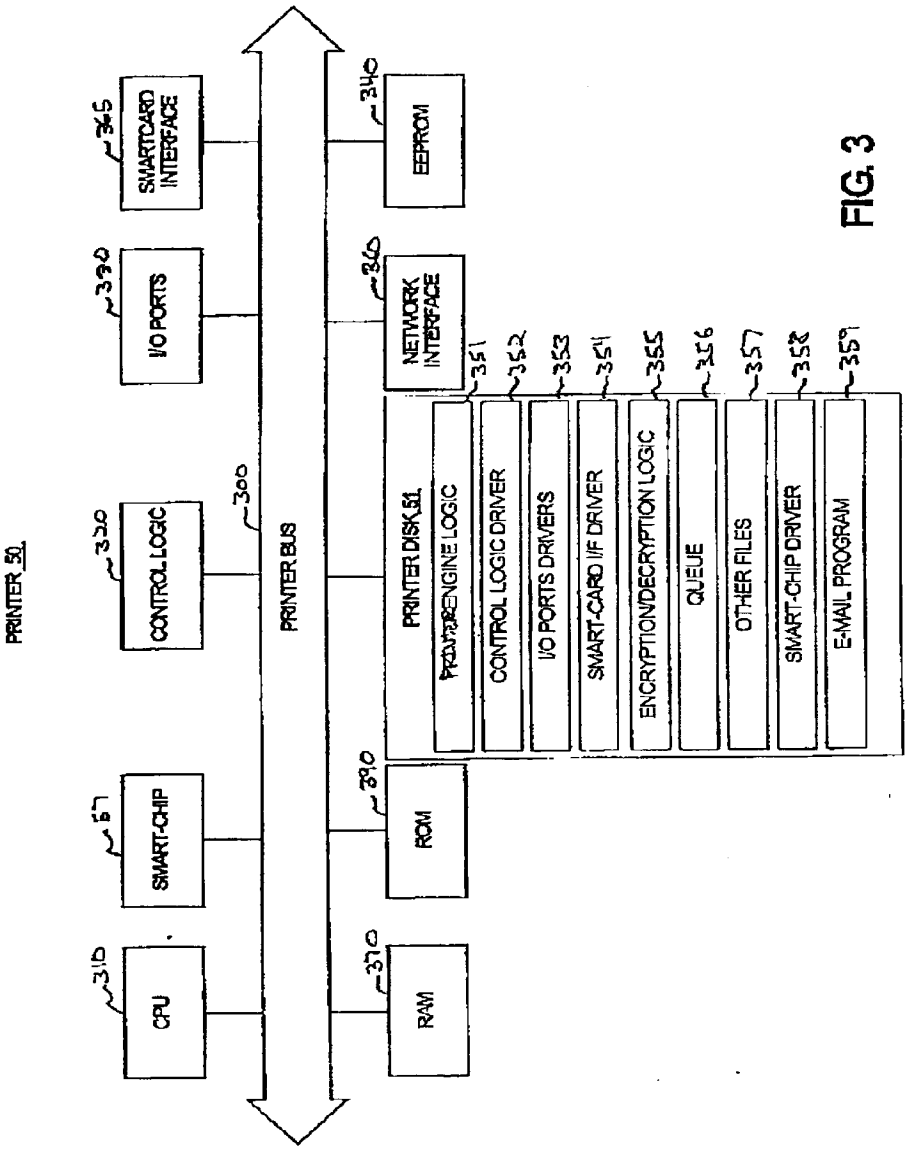

PRINTER 50
PRINTER BUS
300
CPU
310
SMART-CHIP
67
CONTROL LOGIC
320
I/O PORTS
330
SMARTCARD INTERFACE
345
RAM
370
ROM
380
NETWORK INTERFACE
340
EEPROM
340
PRINTER DISK 61
PRINT ENGINE LOGIC
351
CONTROL LOGIC DRIVER
352
I/O PORTS DRIVERS
353
SMART-CARD I/F DRIVER
354
ENCRYPTION/DECRYPTION LOGIC
355
QUEUE
356
OTHER FILES
357
SMART-CHIP DRIVER
358
E-MAIL PROGRAM
359

FIG. 3

【図４】

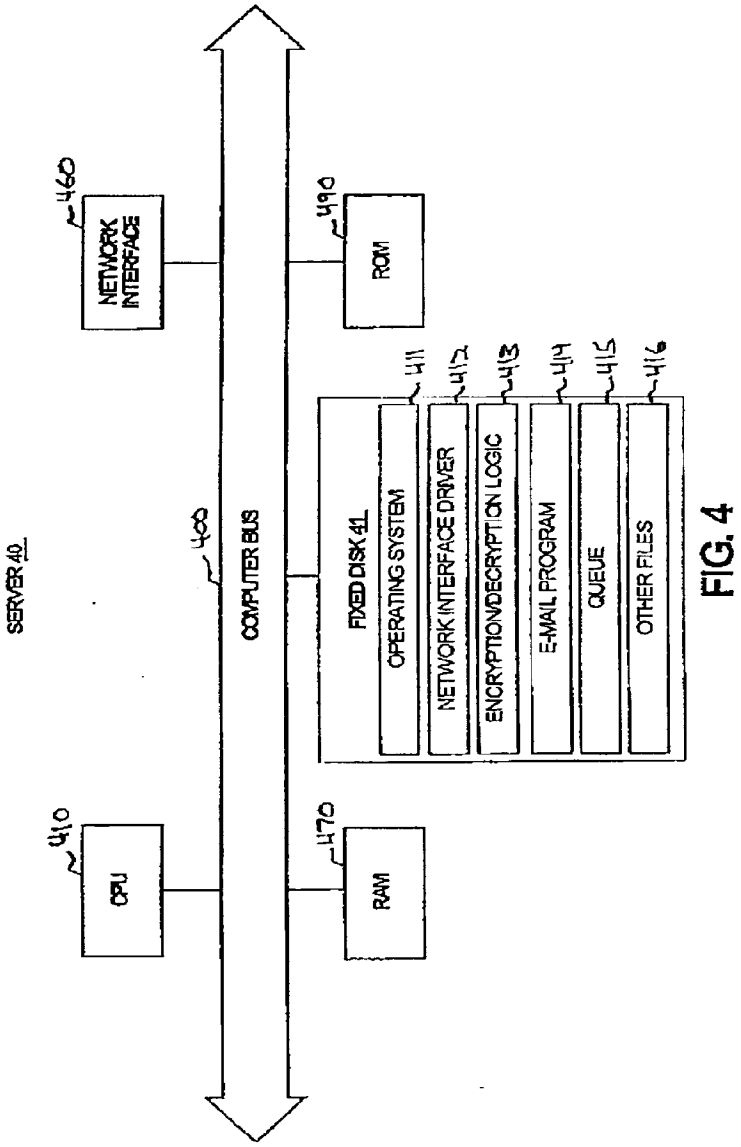

SERVER 40
COMPUTER BUS
400
NETWORK INTERFACE
460
ROM
490
CPU
410
RAM
470
FIXED DISK 41
OPERATING SYSTEM
411
NETWORK INTERFACE DRIVER
412
ENCRYPTION/DECRYPTION LOGIC
413
E-MAIL PROGRAM
414
QUEUE
415
OTHER FILES
416

FIG. 4

【図５Ａ】

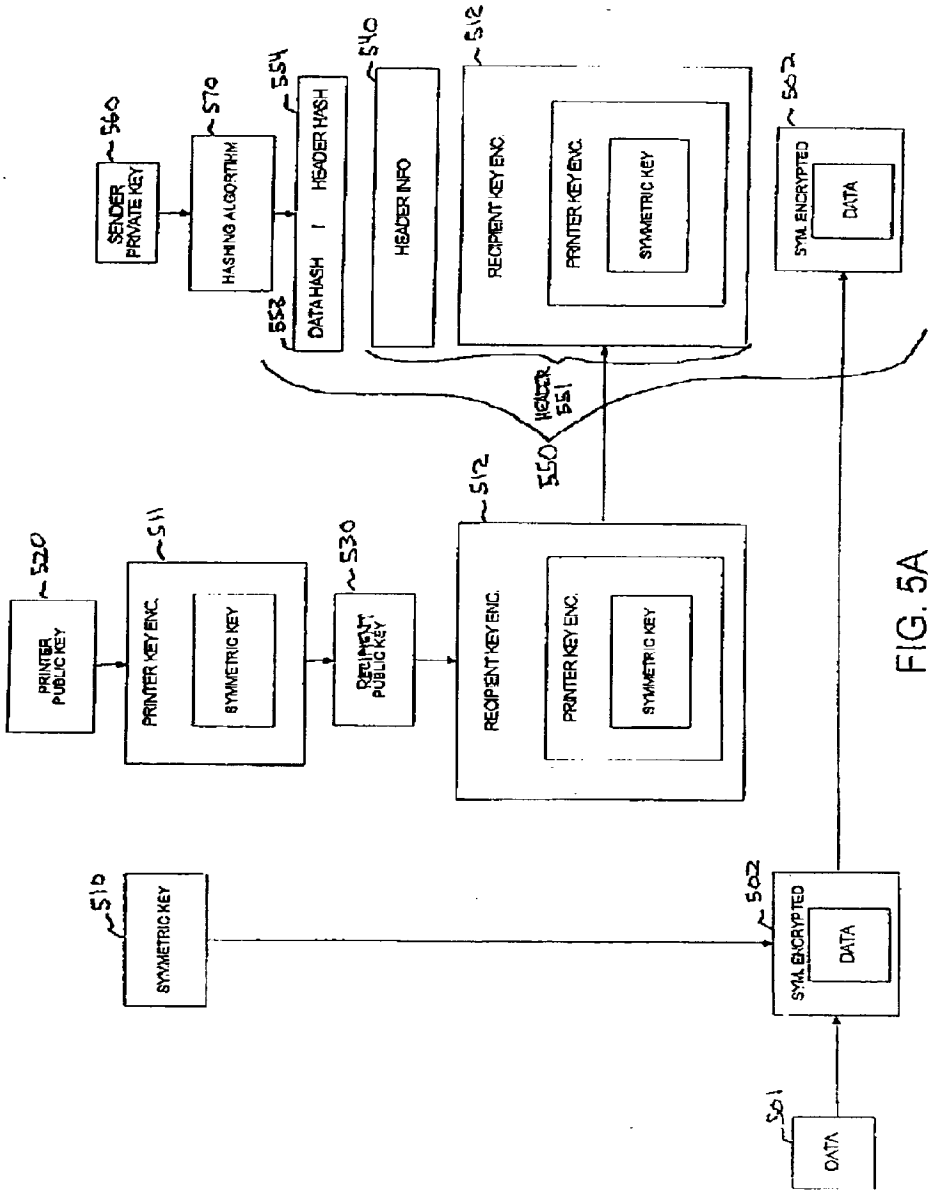

SENDER PRIVATE KEY
560
HASHING ALGORITHM
570
HEADER HASH
554
DATA HASH
552
HEADER INFO
540
RECIPIENT KEY ENC.
PRINTER KEY ENC.
SYMMETRIC KEY
512
SYM. ENCRYPTED
DATA
502
HEADER
551
550
PRINTER PUBLIC KEY
520
PRINTER KEY ENC.
SYMMETRIC KEY
511
RECIPIENT PUBLIC KEY
530
RECIPIENT KEY ENC.
PRINTER KEY ENC.
SYMMETRIC KEY
512
SYMMETRIC KEY
510
SYM. ENCRYPTED
DATA
502
DATA
501

FIG. 5A

【図５Ｂ】

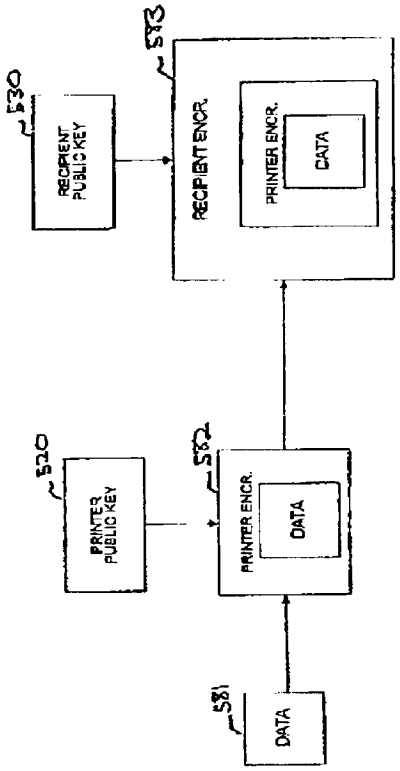

530
RECIPIENT PUBLIC KEY
583
RECIPIENT ENCR.
PRINTER ENCR.
DATA
520
PRINTER PUBLIC KEY
582
PRINTER ENCR.
DATA
581
DATA

FIG. 5B

【図５Ｃ】

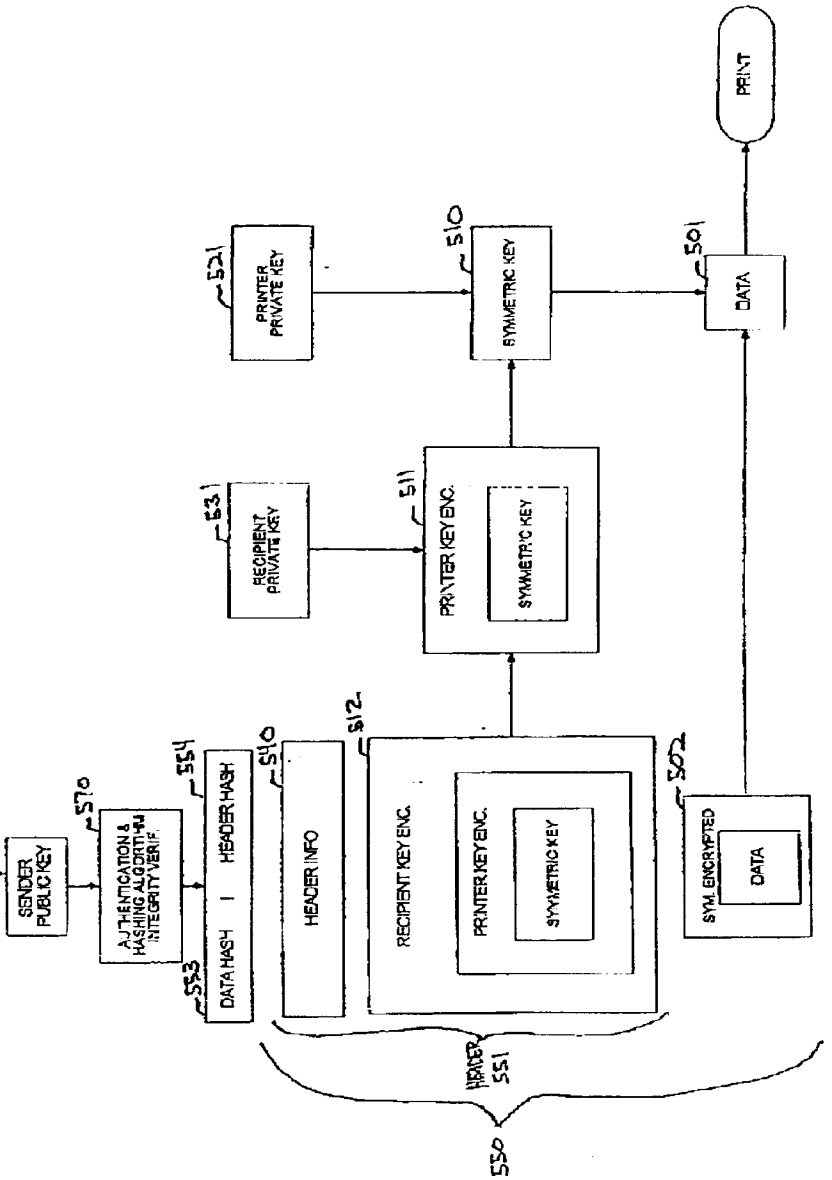

PRINT
DATA
501
SYMMETRIC KEY
510
PRINTER PRIVATE KEY
521
PRINTER KEY ENC.
SYMMETRIC KEY
511
RECIPIENT PRIVATE KEY
531
RECIPIENT KEY ENC.
PRINTER KEY ENC.
SYMMETRIC KEY
512
SYM. ENCRYPTED
DATA
502
HEADER INFO
510
HEADER HASH
554
DATA HASH
553
AUTHENTICATION & HASHING ALGORITHM INTEGRITY VERIF.
570
SENDER PUBLIC KEY
561
HEADER
551
550

FIG. 5C

【図５Ｄ】

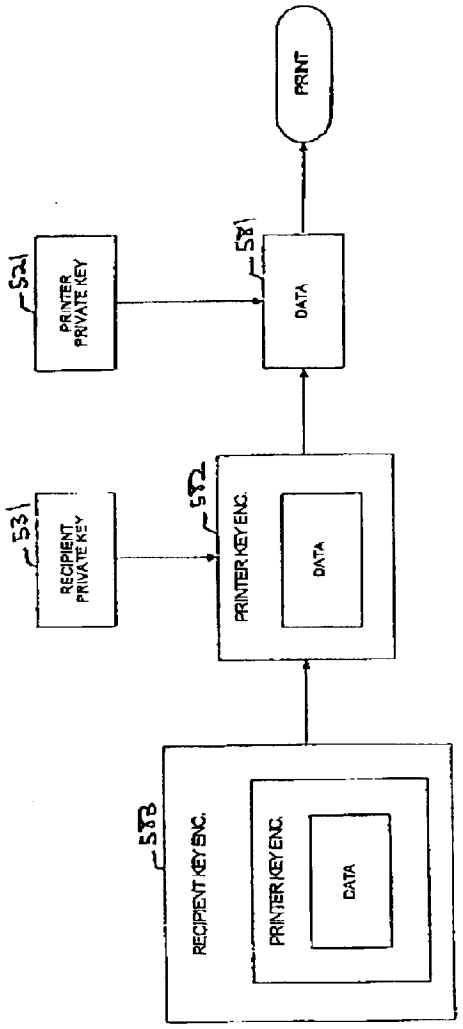

PRINT
PRINTER PRIVATE KEY
DATA
RECIPIENT PRIVATE KEY
PRINTER KEY ENC.
DATA
RECIPIENT KEY ENC.
PRINTER KEY ENC.
DATA

FIG. 5D

【図６】

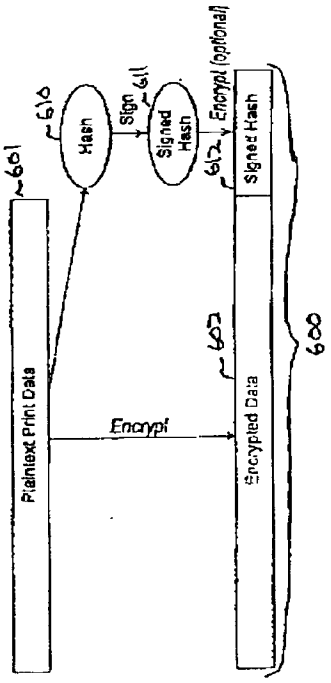

601
615
Hash
Sign
611
Signed Hash
Encrypt (optional)
612
Signed Hash
603
Encrypt
Plaintext Print Data
Encrypted Data
600

FIG. 6

【図７Ａ】

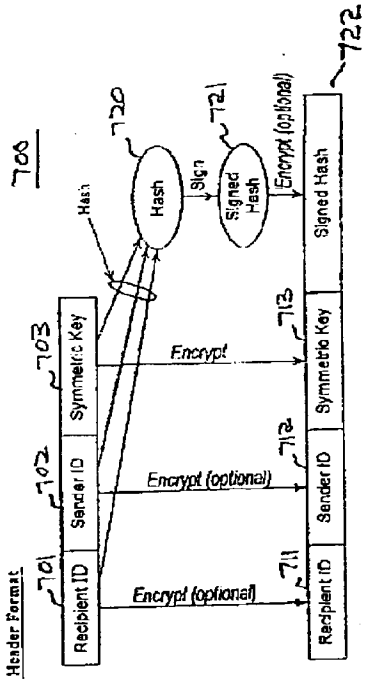

700
Header Format
701
Recipient ID
702
Sender ID
703
Symmetric Key
Hash
720
Hash
Sign
721
Signed Hash
Encrypt (optional)
722
Signed Hash
Encrypt
713
Symmetric Key
Encrypt (optional)
712
Sender ID
Encrypt (optional)
711
Recipient ID

FIG. 7A

【図７Ｂ】

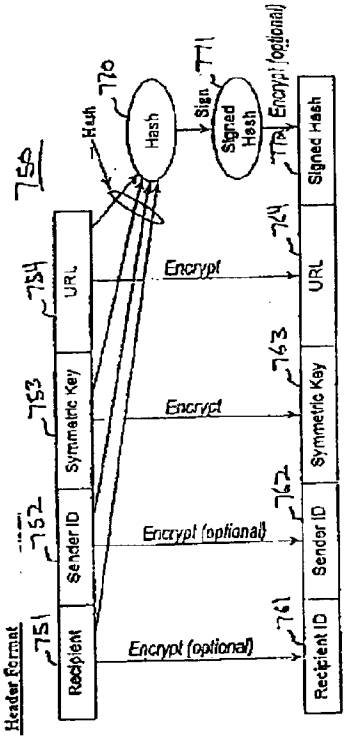

Header Format
755
751
Recipient
752
Sender ID
753
Symmetric Key
754
URL
Hash
770
Hash
Sign
771
Signed Hash
Encrypt (optional)
Encrypt
Encrypt (optional)
Encrypt (optional)
761
Recipient ID
762
Sender ID
763
Symmetric Key
764
URL
Signed Hash

FIG. 7B

【図８】

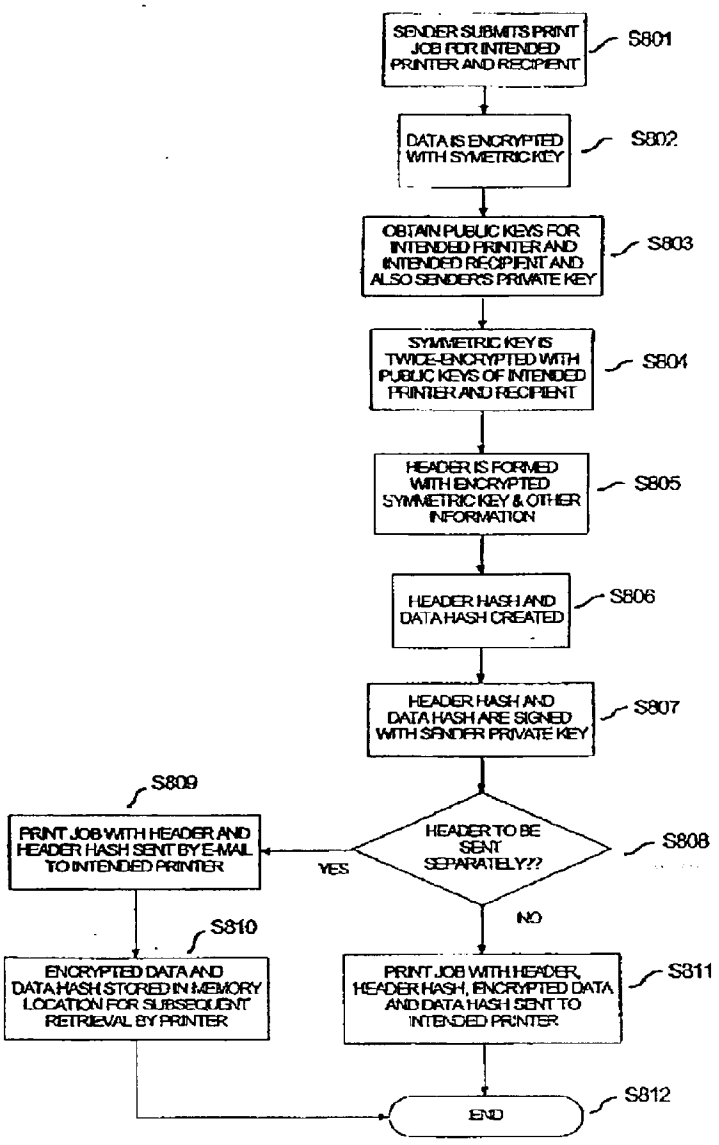
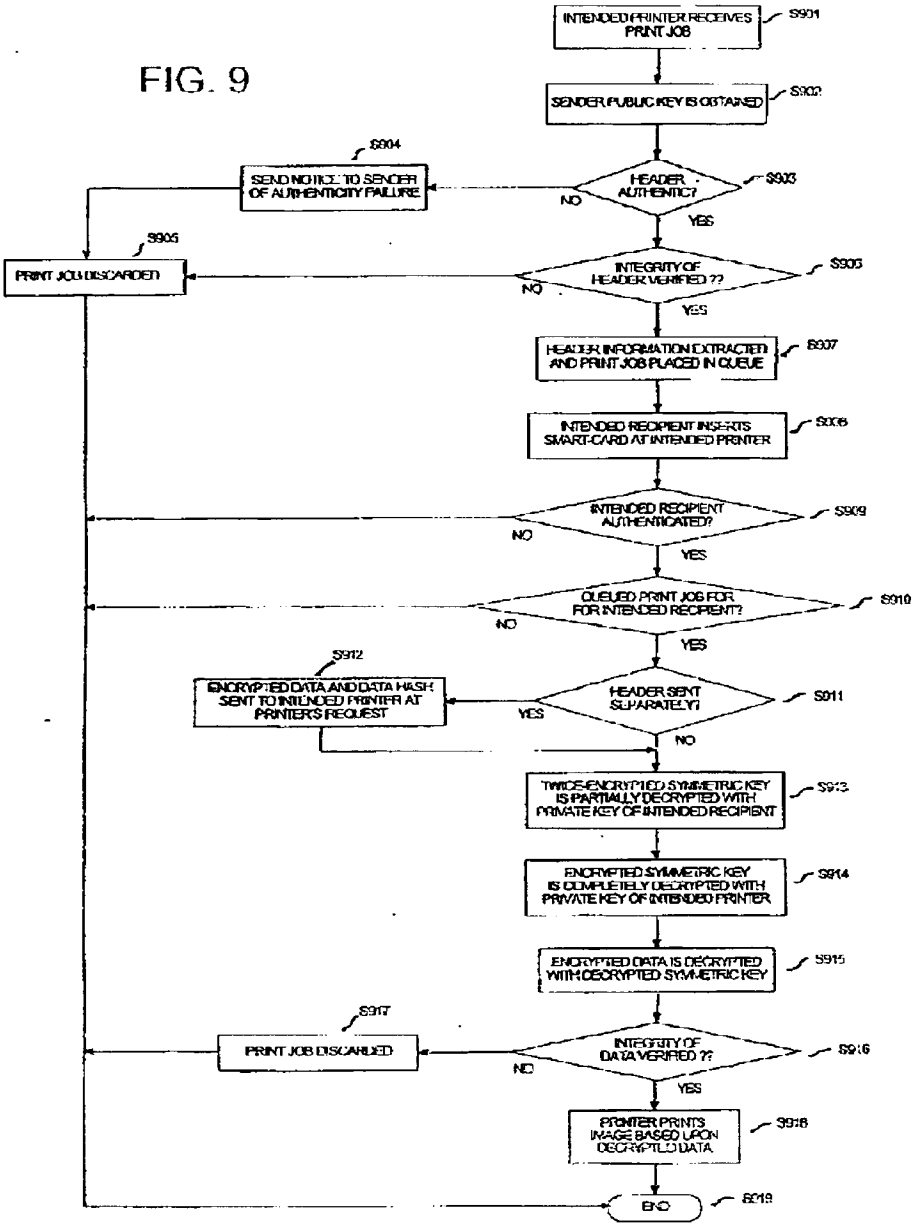

SENDER SUBMITS PRINT JOB FOR INTENDED PRINTER AND RECIPIENT
S801
DATA IS ENCRYPTED WITH SYMETRIC KEY
S802
OBTAIN PUBLIC KEYS FOR INTENDED PRINTER AND INTENDED RECIPIENT AND ALSO SENDER'S PRIVATE KEY
S803
SYMMETRIC KEY IS TWICE-ENCRYPTED WITH PUBLIC KEYS OF INTENDED PRINTER AND RECIPIENT
S804
HEADER IS FORMED WITH ENCRYPTED SYMMETRIC KEY & OTHER INFORMATION
S805
HEADER HASH AND DATA HASH CREATED
S806
HEADER HASH AND DATA HASH ARE SIGNED WITH SENDER PRIVATE KEY
S807
HEADER TO BE SENT SEPARATELY??
S808
YES
NO
PRINT JOB WITH HEADER AND HEADER HASH SENT BY E-MAIL TO INTENDED PRINTER
S809
ENCRYPTED DATA AND DATA HASH STORED IN MEMORY LOCATION FOR SUBSEQUENT RETRIEVAL BY PRINTER
S810
PRINT JOB WITH HEADER, HEADER HASH, ENCRYPTED DATA AND DATA HASH SENT TO INTENDED PRINTER
S811
END
S812

FIG. 8

【図９】

FIG. 9


INTENDED PRINTER RECEIVES PRINT JOB
S901
SENDER PUBLIC KEY IS OBTAINED
S902
HEADER AUTHENTIC?
S903
NO
YES
SEND NOTICE TO SENDER OF AUTHENTICITY FAILURE
S904
PRINT JOB DISCARDED
S905
INTEGRITY OF HEADER VERIFIED ??
S906
NO
YES
HEADER INFORMATION EXTRACTED AND PRINT JOB PLACED IN QUEUE
S907
INTENDED RECIPIENT INSERTS SMART-CARD AT INTENDED PRINTER
S908
INTENDED RECIPIENT AUTHENTICATED?
S909
NO
YES
QUEUED PRINT JOB FOR FOR INTENDED RECIPIENT?
S910
NO
YES
HEADER SENT SUPARATELY?
S911
YES
NO
ENCRYPTED DATA AND DATA HASH SENT TO INTENDED PRINTER AT PRINTER'S REQUEST
S912
TWICE-ENCRYPTED SYMMETRIC KEY IS PARTIALLY DECRYPTED WITH PRIVATE KEY OF INTENDED RECIPIENT
S913
ENCRYPTED SYMMETRIC KEY IS COMPLETELY DECRYPTED WITH PRIVATE KEY OF INTENDED PRINTER
S914
ENCRYPTED DATA IS DECRYPTED WITH DECRYPTED SYMMETRIC KEY
S915
INTEGRITY OF DATA VERIFIED ??
S916
NO
YES
PRINT JOB DISCARDED
S917
PRINTER PRINTS IMAGE BASED UPON DECRYPTED DATA
S918
END
S919

1. Abstract

Secure transmission of data to an intended image output device, wherein the data can be used to generate an image at the intended image output device in the presence of an intended recipient. The data is encrypted using a first key. The first key is then encrypted using a second key and a third key. The second key is a public key of a first private key/public key pair, a private key of the first private key/public key pair being primarily in the sole possession of the intended image output device. The third key is a public key of a second private key/public key pair, a private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image. The encrypted data and the twice-encrypted first key are transmitted to the intended image output device. The twice-encrypted first key is then decrypted by using the private keys of the second and first key pairs, respectively, which are primarily in the sole possession of the intended recipient device and the intended image output device, respectively. The data is then decrypted and printed at an image output device.